DIGITAL FEUDALISM: ENCLOSURES AND ERASURES FROM DIGITAL RIGHTS MANAGEMENT TO THE DIGITAL DIVIDE

Sascha D. Meinrath[†], James W. Losey[‡] & Victor W. Pickard[*]

I.INTRODUCTION

As we enter the second decade of the 21st Century, we find ourselves at a rare historical moment—a time of great opportunity fraught with substantial pitfalls. Numerous potential trajectories of the Internet may unfold before us. While decentralized and participatory platforms have birthed a revived movement for democratized media production, these phenomena depend on the common resource of the Internet; common not in ownership of the integrated networks, but in non-discriminatory access and use of the network.[1] However,

[†] Sascha Meinrath is the Director of the New America Foundation's Open Technology Initiative and is a well-known expert on community wireless networks, municipal broadband, and telecommunications policy. Sascha is a co-founder of Measurement Lab, a distributed server platform for the deployment of Internet measurement tools, and coordinates the Open Source Wireless Coalition, a global partnership of open source wireless integrators, researchers, implementors and companies. Sascha has worked with Free Press, the Cooperative Association for Internet Data Analysis (CAIDA), the Acorn Active Media Foundation, the Ethos Group, and the CUWiN Foundation. The author can be reached at Meinrath@newamerica.net.

[‡] James Losey is a Policy Analyst with the New America Foundation's Open Technology Initiative. He focuses on telecommunications and digital divide issues in the United States and Europe. His work has been published by *Slate, Ars Technica* and *IEEE Spectrum*, as well as numerous policy pieces for the New America Foundation. The author can be reached at Losey@newamerica.net.

[*] Victor Pickard is an assistant professor in the Department of Media, Culture, and Communication at the Steinhardt School of New York University. He received his doctorate from the Institute of Communications Research at the University of Illinois. His research explores the intersections of U.S. and global media activism and politics, media history, democratic theory, and communications policy, and has been published in over two-dozen scholarly journal articles, essays, and book chapters. He is currently finishing a book on the history and future of news media. The author can be reached at vwp201@nyu.edu.

[1] BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 96-97, 387-388 (MIT Press 2010).

as markets evolve, there is a growing uncertainty that policy decisions surrounding the Internet will benefit the general public. Even as social networking and media production have empowered users, less visible structural changes threaten to foreclose many of the Internet's democratic possibilities. Despite the popularity and political power of innovative services like YouTube, Facebook, and Twitter, structural changes threaten to foreclose many of the Internet's democratic possibilities. Furthermore, recent developments in digital rights management ("DRM"), net neutrality, and user privacy reveal unprecedented attacks on basic Internet freedoms.

The Internet ecosystem includes a diverse array of stakeholders who build and depend upon each other's participation. Data transmission depends on access to the physical network, and application functionality depends on the transport of data. As a result, numerous entities—such as network operators and protocol developers—have the power to define the end-user experience. Unfortunately, this ability to intervene can have profound implications for the flow of information, the functionality of applications or hardware, and the specific content or messages allowed over a network. While some scholars continue to herald the brave new world of digital networks,[2] others suggest more cautionary tales of lost opportunities, market failure, and corporate mismanagement.[3] With this tension in mind, this paper examines a number of recent and ongoing Internet policy battles that will determine the future of the Internet's fundamental structures. If history serves as a reliable predictor, these crucial debates will help shape the contours of the Internet for decades, if not generations, to come.

These threats come at an unfortunate time. The U.S. has plummeted in its international rankings on broadband penetration rates in recent years, indicating that something has undermined the participatory ideal of universal broadband connectivity. Not long ago, the U.S. was a leader in Internet adoption.[4] An Oc-

---

[2] *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 2 (Yale Univ. Press 2006). The author notes:

> Together, [technological changes] hint at the emergence of a new information environment, one in which individuals are free to take a more active role than was possible in the industrial information economy of the twentieth century. This new freedom holds great practical promise: as a dimension of individual freedom; as a platform for better democratic participation; as a medium to foster a more critical and self-reflective culture; and, in an increasingly information dependent global economy, as a mechanism to achieve improvements in human development everywhere.

Id.

[3] JEFF CHESTER, DIGITAL DESTINY: NEW MEDIA AND THE FUTURE OF DEMOCRACY 173 (New Press 2007); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 36, 158-160 (Oxford Univ. Press 2006); TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 255-256 (Knopf Press 2010).

[4] *See International Broadband Data*, ORG. FOR ECON. COOPERATION AND DEV. (OECD) (2008), http://www.freepress.net/files/international-broadband-data.pdf (citing data

tober 2000 report by the Danish National IT and Telecom Agency estimated that the United States was "12-24 months ahead of any European Country" in terms of broadband penetration and access.[5] By 2010, the United States slipped to 14th, based on OECD ranking, for overall nationwide broadband penetration, while Denmark was first.[6] These are just a few of the indicators of the worsening digital divide, part of a longer list that we catalog below.

Furthermore, in most markets across the U.S., people must choose between one cable provider and one telephone company for their Internet services.[7] This lack of choice and competition is one of the key reasons that U.S. broadband services currently lag behind a growing number of other industrialized countries and why service is often substandard.[8]

This significant market failure largely accounts for the fact that Americans typically pay several times more a month for a fraction of the broadband speeds available in other countries. In 2010, a typical 50 Mbps connection in the United States cost as much as $145 a month, compared with $60 a month in Japan, $29 a month in South Korea, and $38 month in Hong Kong.[9] In Swe-

---

broadband penetration data available at http://www.oecd.org/dataoecd/63/53/41551452.xls).

[5] EIRWEN NICHOS, ZETA TSATSANI & ELIZABETH HARDING, THE STATUS OF BROADBAND ACCESS SERVICES FOR CONSUMERS AND SMES 4 (Oct. 2000), *available at* http://en.itst.dk/policy-strategy/publications/the-status-of-broadband-access-services-for-consumers-and-smes/The%20status%20of%20broadband%20access%20services%20for%20consumers%20and%20SMEs.pdf.

[6] *See OECD Broadband Statistics – OECD Fixed Broadband Subscriptions Per 100 Inhabitants June 2010*, ORG. FOR ECON. COOPERATION AND DEV., http://www.oecd.org/dataoecd/21/35/39574709.xls (last visited May 14, 2011).

[7] The National Broadband Plan released by the Federal Communications Commission notes that 96% of Americans have a choice of 2 or fewer wireline broadband providers. *See* FED. COMMC'NS COMM'N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 37 (2010), *available at* http://www.broadband.gov/download-plan [hereinafter NATIONAL BROADBAND PLAN].

[8] *See* YOCHAI BENKLER, HARVARD BERKMAN CTR FOR INTERNET AND SOC'Y 36 (2010) [hereinafter BERKMAN REPORT], *available at* http://cyber.law.harvard.edu/pubrelease/broadband; JAMES LOSEY & CHIEHYU LI, NEW AMERICA FOUNDATION, PRICE OF THE PIPE: COMPARING THE PRICE OF BROADBAND SERVICE AROUND THE GLOBE 1-2 (April 2010) (stating that a "[l]ack of competition is a major factor influencing the higher prices and slower speeds found in the U.S" and that "prices are higher when only one or two providers are available."), *available at* http://www.newamerica.net/sites/newamerica.net/files/policydocs/Price%20of%20the%20Pipe_0.pdf . Internet service is also the third most common consumer complaint received by the Federal Trade Commission. *See* Press Release, Fed. Trade Comm'n , FTC Releases List of Top Consumer Complaints in 2010; Identity Theft Tops the List Again (Mar. 8, 2011) (*available at* http://www.ftc.gov/opa/2011/03/topcomplaints.shtm).

[9] JAMES LOSEY & CHIEHYU LI, NEW AMERICA FOUNDATION, PRICE OF THE PIPE: COMPARING THE PRICE OF BROADBAND SERVICE AROUND THE GLOBE 1-2 (April 2010), *available at* http://www.newamerica.net/sites/newamerica.net/files/policydocs/Price%20of%20the%20Pipe_0.pdf.

den, open access networks have created vibrant competitive markets, as evidenced by the drop in price for 100 Mbps symmetric lines to $46/month in Stockholm.[10] These figures and other studies[11] suggest that Americans could have access to faster, cheaper broadband connectivity if the U.S. implemented similar open policies. When the marketplace fosters competition, prices drop and broadband speeds increase dramatically.

The cost and availability of broadband is only a part of the dilemma. Network operators further contribute to the problem by resisting the implementation of network management techniques that increase capacity, choosing instead to ration "existing capacity among competing network users or uses."[12] In the U.S., users might share a local node with over two hundred other connections,[13] and experience average speeds that are half the advertised price.[14]

If these trends continue, the Internet will devolve into a feudalized space—one that limits democratic freedoms while enriching an oligopoly of powerful gatekeepers. This article illuminates the specific policy debates connected to these vulnerabilities, while uncovering normative understandings about the role of the Internet in a democratic society. Using the seven-layer OSI model as a framework, our analysis catalogs current threats to this telecommunications commons and examines the policy provisions that should be implemented to prevent the feudalization of the Internet. By cataloging current threats to a democratic Internet and closely examining the linkages between intersecting policy battles, this paper illuminates both what is at stake and what policy pro-

---

[10] *Id.*

[11] *See* BERKMAN REPORT, *supra* note 8, at 13. As Benkler concludes,

> Our most surprising and significant finding is that 'open access' policies—unbundling, bitstream access, collocation requirements, wholesaling, and/or functional separation—are almost universally understood as having played a core role in the first generation transition to broadband in most of the high performing countries; that they now play a core role in planning for the next generation transition; and that the positive impact of such policies is strongly supported by the evidence of the first generation broadband transition. The importance of these policies in other countries is particularly surprising in the context of U.S. policy debates throughout most of this decade. While Congress adopted various open access provisions in the almost unanimously-approved Telecommunications Act of 1996, the FCC decided to abandon this mode of regulation for broadband in a series of decisions beginning in 2001 and 2002. Open access has been largely treated as a closed issue in U.S. policy debates ever since.

Id.

[12] *See* Benjamin Lennett, *Dis-Empowering Users vs. Maintaining Internet Freedom: Network Management and Quality of Service (QoS)*, 18 COMMLAW CONSPECTUS 97, 146 (2009).

[13] *Id.* at 117.

[14] *See* NATIONAL BROADBAND PLAN, *supra* note 7, at 21; *see also* Fed. Commc'ns Comm'n, *Broadband Performance* 4 (Fed. Commc'ns Comm'n, OBI Technical Paper No. 4, 2010), *available at* http://download.broadband.gov/plan/fcc-omnibus-broadband-initiative-%28obi%29-technical-paper-broadband-performance.pdf.

visions should be implemented to prevent the feudalization of the Internet.

Part II introduces the concept of feudalization—the structural transformations through which public space becomes controlled by private interests—and how the OSI stack can be used to understand the hierarchical dependencies of networked technology. Part III explores policy enabled enclosure at different layers of the OSI stacks and illustrates how control of any one layer can be leveraged to enclose other layers and the Internet. Part IV makes the case for open technologies in light of the implications created by closed technologies at different layers of the Internet. Having established the potential for open technologies to preserve the Internet as a commons, in Part V we offer policy solutions to the various examples of enclosures in Part III. Part VI concludes with the case for a new policy paradigm that recognizes the need to address issue across the technological stack in order to protect the democratic potential of the Internet.

II. THE FEUDALIZATION OF PUBLIC SPACE AND THE ART OF ENCLOSURE

The popular metaphor of the Internet as a public sphere often overlooks the darker side of this formulation. In discussing the structural transformations of the public sphere, Jürgen Habermas clarified that while the market helped create the initial space for civic engagement, it also constantly threatened to colonize public spheres through privatization.[15] He referred to this phenomenon as the "re-feudalization of the public sphere," a process in which the newly created public space would succumb to commercial pressures and reorganize along familiar power hierarchies.[16] In recent years, Habermas has increasingly underscored the risk of market colonization, decrying the tendency toward treating the public sphere as merely another location for commercial relations to take hold.[17]

A similar phenomenon, by analogy, is "enclosure," a process by which private interests overtake common or public lands for the purpose of exploiting the lands to the exclusion of others.[18] In the 15th and 16th centuries, the Eng-

---

[15] *See generally* JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE (TRANS. T. BURGER) (MIT Press 1989).

[16] *Id.*

[17] Jürgen Habermas, *Political Communication in Media Society - Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research*, 16 COMM. THEORY 411, 412 (2006).

[18] *See* James Boyle, *Enclosure and the Disappearance of the Public Domain*, 131 DAEDALUS 2, 13-17 (2002) (analyzing the English enclosure movement's economic principles and how they can be used to explain the modern era's DMCA and other electronic data regimes).

lish countryside witnessed a sudden privatization of land that had long been treated as a commons. This change in the legal standing of the land criminalized a range of behavior that had previously been accepted as cultural norms, such as maintaining livestock and harvesting food or gleaning on common lands.[19] With the advent of poor laws, these behaviors were suddenly recategorized as poaching. Similarly, in the online context, enclosure systematically removes resources out of the public sphere and replaces a general notion of maximizing the public good with a logic of profit maximization, thus excluding the majority of people and furthering the profits of a minority.

Debates over digital commons often assume a false dichotomy by treating digital goods as traditional commodities. Most commodities are rivalrous—their use by one entity excludes their use by another. For example, if one consumes a fish, then that fish is not available to anyone else: there is a natural rivalry among consumers for access to these goods. Likewise, most rivalrous goods are excludable—one can prevent other consumers from eating the fish by charging a price for it (thus laying the foundation for the traditional "Economics 101" assumption that pricing will seek equilibrium between supply and demand). Another foundational pillar of this traditional thinking is that non-rivalrous goods are also non-excludable; that it is impossible to stop an individual from utilizing this resource (e.g., daylight, air, learning). In addition, rivalrous, yet non-excludable goods have given rise both to the "commons" and the dystopian "tragedy of the commons," exemplified by problems like overfishing, overgrazing, and pollution of the environment.

	Excludable	**Non-Excludable**
Rivalrous	Private Goods	Common Goods
Non-rivalrous		Public Goods

What is at stake in this increasingly feudalized space is a shifting concept of ownership. What happens when public goods and common goods are re-envisioned as private goods? And how do regulatory processes and technological innovations spur these shifts? The "digital commons" metaphor may serve as a poignant reminder that the Internet's unique power has rested largely on its openness, on the fact that it is our most public media, and that it was created as a result of public support through DARPA and other tax-supported entities,

[19] DAN SCHILLER, DIGITAL CAPITALISM: NETWORKING THE GLOBAL MARKET SYSTEM 77 (MIT Press 1999).

but it oversimplifies the multi-layered nature of the technology and the potential for enclosures to manifest themselves in seemingly innocuous ways. Built using a "dumb" infrastructure,[20] the Internet has been defined by protocols that transfer data packets on a "first-in first-out," best-effort basis. The success of the Internet has been defined by the range of uses and application freedoms facilitated by its openness. Under this framework, application usage by two users with access to bandwidth (such as neighbors both subscribing to 5 Mbps connections), or two viewers watching the same online video, is *de facto* non-rivalrous. However, as the fundamental structures of the Internet undergo transformation, its non-rivalrous nature is quickly being supplanted by the same forces that drove wedges and created power pyramids in the English countryside in the 14th Century. The freedom to define the Internet to the needs of the user, to share video, and to choose the appropriate method of communication over TCP/IP is quickly becoming enclosed.

A. Critiquing the Internet

An expanding corpus of research describes areas where corporate encroachment is already occurring. One of the best known examples is renounced scholar Lawrence Lessig's distinction between read-only culture and rewritable culture, where he notes that creativity is sacrificed for private profits as an intellectual policy regime runs amok.[21] Economist Michael Perelman makes a similar argument that the public domain's digital commons are undergoing a kind of enclosure and becoming increasingly impoverished by a proprietary mentality.[22]

Other scholars highlight the Internet's transformation at the network operation and content layers.[23] In *The Future of Ideas,* Lessig listed the threats gatekeeping Internet service providers (ISPs) pose for the Internet.[24] One recent article by Bart Cammaerts categorized these criticisms as falling along struc-

---

[20] *See* David Isenberg, *Rise of the Stupid Network,* http://www.hyperorg.com/misc/stupidnet.html (last visited May 14, 2011) (explaining how the "stupid network" consists of a "dumb transport in the middle, and intelligent user-controlled endpoints" as well as a design "guided by plenty, not scarcity").

[21] *See generally* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (Penguin Books 2004).

[22] MICHAEL PERELMAN, STEAL THIS IDEA: INTELLECTUAL PROPERTY RIGHTS AND THE CORPORATE CONFISCATION OF CREATIVITY (Palgrave 2002).

[23] *See* MARTIN FRANSMAN, THE NEW ICT ECOSYSTEM: IMPLICATIONS FOR EUROPE 52-54 (Kokoro 2007); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 67-69 (Yale Univ. Press 2008); WU, *supra* note 3, at 289-290; VAN SCHEWICK, *supra* note 1, at 84-88.

[24] LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (Vintage Books 2002).

tural or individual levels.[25] This analysis focuses on enclosure tactics that are more structural in nature (as opposed to the ways in which content providers have become increasingly commercial in recent years). Though some attempts have been directed toward these areas, relatively few efforts have tried to systematically model the various critiques or try to connect them to larger systemic analyses. While many of these critiques deal with the oft-mentioned "digital divide" and focus on issues related to access, other critiques emphasize deeper systemic issues.

Dan Schiller leveled one of the first critiques aimed at delineating the neoliberal shift in market expansion and political economic transition encompassing the Internet, which he called "Digital Capitalism."[26] Schiller noted that Internet networks increasingly serve the aims of transnational corporations via strict privatization of content and unregulated transborder data flow allowing content owned within one region to enter new markets.[27] Likewise, he advocates for the creation of a "communications commons," and efforts towards the "financing of a multiplicity of decentralized but collectively or cooperatively operated media outlets, licensed on the basis of commitment to encouraging participatory involvement in all levels of their activity" to "more fully [release] the democratic and participatory potential of digital technologies."[28] These critical trends presaged a growing body of work that addresses normative concerns like open architecture, open access, and online ethics. For example, Professor Yochai Benkler's *Wealth of Networks* advocates for a commons based policy orientation. This approach is aligned with the notion of Cooper's "open architecture."[29] Frequently referred to as a commons-based approach to the management of communications systems, this model emphasizes cooperation and innovation as opposed to privatization and enclosure.

More recently, Jonathan Zittrain has intervened in these debates to argue that the U.S. is allowing the Internet conform to connect appliances rather than

---

[25] Bart Cammaerts, *Critiques on the Participatory Potentials of Web 2.0*, COMMUNICATION, CULTURE & CRITIQUE 358, 336-362 (2008), *available at* http://eprints.lse.ac.uk/23770/1/Critiques_on_the_participatory_potentials_of_Web_2.0_%28LSERO%29.pdf.

[26] SCHILLER, *supra* note 19, 204-207.

[27] *Id.* at xvi.

[28] *Id.* at 204-205.

[29] Mark Cooper, *Making the Network Connection, Using Network Theory To Explain The Link Between Open Digital Platforms And Innovation*, *in* OPEN ARCHITECTURE AS COMMUNICATIONS POLICY, CENTER FOR INTERNET AND SOCIETY STANFORD LAW SCHOOL 126 (Mark Cooper ed., 2004), *available at* http://cyberlaw.stanford.edu/attachments/openarchitecture.pdf. Cooper writes: "The Internet is a "stack" of protocols whose architecture is open. In other words, the digital communications platform is a nested set of open components that exhibit an unprecedented level of connectivity. It exhibits the modular, hierarchical, distributed, multiscale connectivity of an ultrarobust network."

produce generative technology.[30] Zittrain sees the development of the Internet as a history of lost opportunity. To underscore this shift, he uses a three part layered model that distinguishes between physical, protocol and application layers. He also allows for content and social layers above these three.[31] Although this model is useful for highlighting areas of enclosure—and provides yet another typology for understanding different theories of technology—we prefer an adaptation of an older schematic that has been utilized as both the foundation of the Internet and has the advantage of highlighting certain aspects of the Internet that other models fail to capture: the OSI model.

B. The OSI Model

Developed by the International Standardization Organization, the seven-layer OSI (Open Systems Interconnection) model breaks communications network into different layers, with each layer representing different core functions of the network.[32] A hierarchical architecture, the range of function of different layers of the stack is maximized by the openness of the surrounding layers.

The OSI model serves as a convenient framework for illustrating various threats to Internet. Although digital feudalism is not limited to the threats at the OSI layers—and although the OSI model is not a strict cross section of the Internet—the model is a useful heuristic for documenting encroachments at individual layers. Most importantly, the OSI model helps illustrate how sufficient control at a single layer can enclose the Internet commons and limit end-user freedoms.

---

[30] *See* ZITTRAIN, *supra* note 23, at 2-4. For example, Zittrain draws a distinction between the early Apple II and modern iPhone systems, noting that the Apple II was "generative technology" where Apple did not specify a specific use for the platform.

[31] *See* ZITTRAIN, *supra* note 23, 67-68.

[32] *See X.200 : Information technology - Open Systems Interconnection - Basic Reference Model: The basic model*, INT'L TELECOMS UNION, http://www.itu.int/rec/T-REC-X.200/en/.

Open Systems Interconnection Basic Reference Model[33]

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment	4. Transport	End-to-end connections and reliability
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing (MAC & LLC)
	Bit	1. Physical	Media, signal and binary transmission

III. ENCLOSURES ALONG OSI DIMENSIONS

A. Physical Layer Problems

The physical layer is the foundational layer of networks. The transport mediums that comprise the physical layer—copper and fiber, switches, routers, and slices of radio spectrum—can be open or closed. Regulatory and legal intervention plays an important role in defining the limits at the physical layer, and in turn, what methods and technologies can be used to communicate through on the network.

For example, without the advent of the FCC's landmark Carterfone decision

---

[33] *OSI Model,* WIKIPEDIA, http://en.wikipedia.org/wiki/OSI_model (last visited May 14, 2011); *see* PATRICK CICCARELLI & CHRISTINA FAULKNER, NETWORKING FOUNDATIONS 16-34 (2004).

to allow interconnection of "foreign attachments" to the AT&T telephone network, wireline communications may well have taken a different turn—even preventing the emergence of the Internet in its present form. Prior to Carterfone, the FCC tariff governing interconnecting devices stated, "No equipment, apparatus, circuit or device not furnished by the telephone company shall be attached to or connected with the facilities furnished by the telephone company, whether physically, by induction or otherwise."[34] Even the Hush-a-Phone, a plastic attachment that blocked room noise, was originally deemed illegal to affix to telephone handsets.[35]

While AT&T may have wanted end-to-end control over every part of their telephone network, the FCC wisely concluded that end-users should decide for themselves which devices and technologies to attach to telephone lines. In doing so, it created a legal precedent that facilitated the development of foreign attachments,[36] such as office telephone systems, answering machines, and—most importantly—the computer modem. Unfortunately, next-generation networking systems may not be so lucky, as AT&T and other incumbents threaten to recreate the pre-Carterfone conditions that existed over 40 years ago on today's wireless networks.

1. Open Access & Common Carriage

In addition to the mandate to allow "foreign attachments" on the telephone network, two key elements fueled the establishment and growth of the Internet: open access and common carriage. Open access policies required "existing carriers to lease access to their networks to their competitors, mostly at regulated rates."[37] Open Access meant that anyone could create an Internet Service Provider (ISP), and AT&T had to provide access to facilities and interconnection for these new rivals. In addition, because it was subject to common carriage requirements, AT&T had to provide connectivity over its own network between end-users' computer modems and these new competitive ISPs. In many regards, these key factors are what helped the Internet develop into "a network of networks," as opposed to a singular system controlled by one entity.

However, policies supported by incumbent network operators have system-

---

[34] *In re* Use of the Carterfone Device in Message Toll Telephone Service, Thomas F. Carter and Carter Electronics Corp., Dallas, Tex. (Complainants), v. American Telephone and Telegraph Co., Associated Bell System Companies, Southwestern Bell Telephone Co., and General Telephone Co. of the Southwest (Defendants), *Decision*, 13 F.C.C.2d 420, 421 (June 26, 1968) [hereinafter *Carterfone Decision*].

[35] *See* LESSIG, *supra* note 24, at 30.

[36] *Id.* at 421.

[37] BERMKAN REPORT, *supra* note 11 at 14.

atically eroded these provisions. The Telecommunications Act of 1996 codified a binary classification of telecommunications services and information services, subjecting the former to common carriage and unbundled access at reasonable rates.[38] However, this binary classification broke down as technological convergence offered the same service over previously distinctly different legacy technologies, such as the telephone and cable television.[39] Further, the 1996 Act did not address IP-based voice services (e.g., VoIP) as a telecommunications or information service, .

Changes in the regulatory framework for broadband Internet service has benefitted a handful of ISPs at the expense of the greater market. On June 27, 2005, the Supreme Court's *Brand X* decision upheld the authority of the FCC to reclassify cable broadband service as an "information service."[40] Because they were not subject to common carriage provisions, cable ISPs were not required to offer access to third-party ISPs. Conversely, DSL incumbents , as a telecommunications services, had to allow ISPs, including competing cable providers, access to its own infrastructure. MCI argued that this provided an unfair competitive advantage to the cable ISPs.[41] Soon thereafter, the FCC ruled that digital subscriber line (DSL) ISPs and others were no longer required to unbundle their services or sell network access to potential competitors.[42]

Since these deregulatory decisions, broadband competition in the United States has collapsed. According to the U.S. Census, nearly 50% of independent ISPs went out of business between 2000 and 2005, during which time the U.S.'s international broadband rankings plummeted.[43] The National Broadband

---

[38] Telecommunications Act of 1996, 47 U.S.C. 251 (c)(3) (2006).

[39] *See* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 25-26, 209-10 (2005) (discussing the obsolescence of the Communications Act of 1934, as amended in 1996, because its structure does not match the structure of services as they are delivered over the Internet today).

[40] *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs. (*Brand X*), 545 U.S. 967, 968-969 (2005); *see also In re* Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, Internet Over Cable Declaratory Ruling, Appropriate Regulatory Treatment for Broadband Access to the Internet over Cable Facilities, *Declaratory Ruling & Proposed Rulemaking*, 17 F.C.C.R. 4798, 4841-42 (Mar. 14, 2002).

[41] *Brand X*, 545 U.S. at 1000.

[42] *In re* Appropriate Framework for Broadband Access Over Wireline Facilities, *Report & Order & Notice of Proposed Rulemaking*, 20 F.C.C.R. 14866, 14904 (Aug. 5, 2005).

[43] In 2000, the U.S. Census Bureau Statistics of U.S. Business listed 9,335 ISPs in the United States. *See Number of Firms, Number of Establishments, Employment and Annual Payroll by Employment Size of the Enterprise for the United States, All Industries 2000*, U.S. CENSUS BUREAU, http://www2.census.gov/econ/susb/data/2000/us_6digitnaics_2000.xls). By 2005 the number of ISPS was 4,417. *See Number of Firms, Number of Establishments, Employment and Annual Payroll by Employment Size of the Enterprise for the United States, All Industries*

Plan, released in March 2010, indicated that only 4% of Americans have a choice of more than two wireline Internet service providers.[44] The lack of competition in the market contributes to both the slow speeds and high costs of wireline connectivity in the United States. Unfortunately, when it comes to wireless communications, the prognosis may be even worse.

2. Spectrum Resources

Spectrum capacity is essential for wireless networks, but current licensing and distribution schemes are archaic and hyper-inefficient. Current spectrum allocation models assume that single entities require absolute control over their spectrum band at all times, resulting in gross inefficiencies of spectrum allocation.[45]

Between January 2004 and August 2005, the National Science Foundation commissioned six reports from Shared Spectrum[46] looking at actual spectrum use in six cities across the United States—their results showed that the amount of spectrum actually being used as pitifully low[47]:

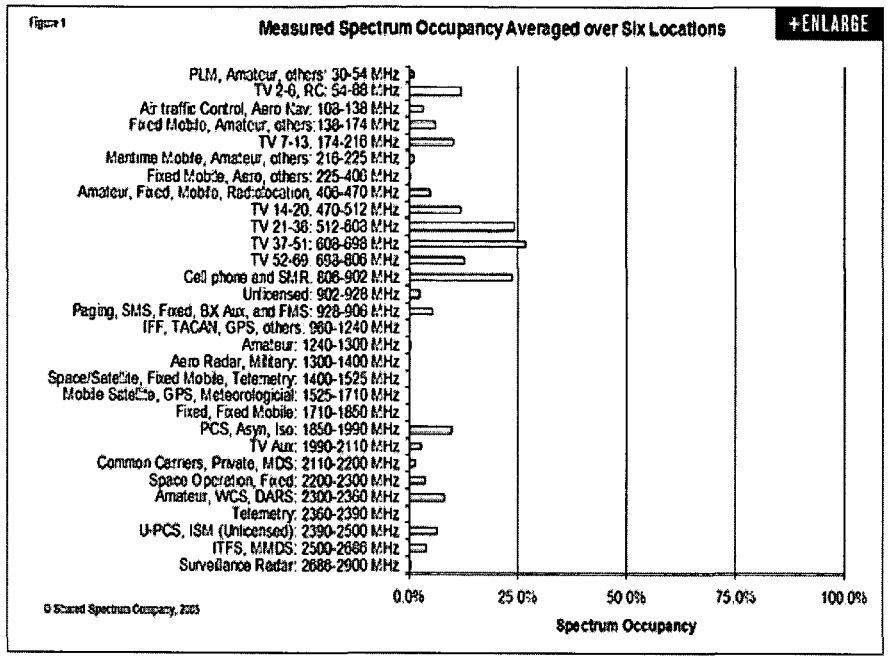
2005, U.S. CENSUS BUREAU, http://www2.census.gov/econ/susb/data/2005/us_6digitnaics_2005.xls.

[44] NATIONAL BROADBAND PLAN, *supra* note 7, at 37.

[45] *See* Pickard & Meinrath, *supra note* 17.

[46] All six spectrum usage reports are available at *SSC*, SHARED SPECTRUM, http://www.sharedspectrum.com/papers/spectrum-reports/ (last visited May 14, 2011) [hereinafter *Spectrum Usage Reports*].

[47] *See* MARK A. HENRY, ET AL., SHARED SPECTRUM COMPANY, SPECTRUM OCCUPANCY MEASUREMENTS CHICAGO, ILLINOIS 48 (2005), *available at* http://www.sharedspectrum.com/wp-content/uploads/NSF_Chicago_2005-11_measurements_v12.pdf.



The overall results of this analysis was of the sites surveyed, spectrum occupancy was highest in Chicago, Illinois, with 17.4% of the frequencies in use, and that the average utilization rate was 5.2%.[48] In their most recent study of spectral efficiency in 2007, they conducted measurements in Limestone, Maine, and found a usage rating of 1.7%.[49] Furthermore, today, over 95 percent of the public airwaves (under 30 GHz) are either reserved for governmental use or licensed to private parties.[50] Given these real-world measurements, it is shocking that there are so few opportunities to access the public airwaves, especially when access to clearly underutilized spectrum would assist in the development of innovative new technologies that benefit the public and expand communication opportunities.

---

[48] *Id.* at 48-49, 53.

[49] TUGBA ERPEK, MARK LOFQUIST & KEN PATTON, SHARED SPECTRUM COMPANY, SPECTRUM OCCUPANCY MEASUREMENTS LORING COMMERCE CENTRE LIMESTONE MAINE 37 (2007), *available at* http://www.sharedspectrum.com/wp-content/uploads/Loring_Spectrum_Occupancy_Measurements_v2_3.pdf.

[50] In cases like the citizens' band (CB) spectrum is set aside for amateur use, or according to "Part 15" rules which allow some public wireless devices such as garage door openers and microwave ovens to operate in unlicensed spectrum. *See* BENNETT Z. KOBB, WIRELESS SPECTRUM FINDER: TELECOMMUNICATIONS, GOVERNMENT AND SCIENTIFIC RADIO FREQUENCY ALLOCATIONS IN THE US 30 MHZ-300 GHZ (McGraw-Hill 2001), and NAT'L TELECOMM AND INFO. ADMIN., MANUAL OF REGULATIONS AND PROCEDURES FOR FEDERAL RADIO FREQUENCY MANAGEMENT (REDBOOK) (US Gov't Printing Office, 2008).

Spectrum allocation and frequency assignments largely ignore today's technical realities and gross inefficiencies of spectrum usage currently exist. The current spectrum allocation regime ignores technologies such as cognitive radios, which adapt to available space in real-time in order to permit concomitant use of spectrum by unlicensed and licensed users.[51] Instead, the FCC and NTIA licensing model is predicated on use of the public airwaves dating back to the World War I era that is "woefully outdated given current technologies and spectrum needs."[52] This "command and control" approach to spectrum management allows only a single entity to broadcast on a given frequency, often at a specific power level and geographic location.[53] Tim Wu has likened these command and control policies to "Soviet Style Rules . . . dating from the 1920s."[54] Wu estimates that "[a]t any given moment, more than 90 percent of the nation's airwaves are empty,"[55] and other analysts have referred to current spectrum management policy as a "paradigm for economic inefficiency."[56]

This licensing scheme benefits the holders of exclusive licenses. Incumbent interests already invested in licensed frequencies seek to prevent competition by maintaining the antiquated regulatory status quo.[57] In this way, incumbents dramatically slow down change or stop it altogether. "Among neutral observers," Nuechterlein & Weiser note, "there is little dispute that . . . the current spectrum regime requires a comprehensive overhaul."[58] In other words, from a digital feudalism perspective, those who have control over the physical layer of the OSI model can impede competitors, lock customers into expensive service tiers, and inhibit innovation.

B. Data Link and Network Layer Problems

The second OSI layer, the data link layer, creates the foundation for TCP/IP transmission, creating the framework for additional protocols, like UDP, to communicate by transferring data between different network components.[59]

---

51 Sascha Meinrath & Victor W. Pickard, *Revitalizing the Public Airwaves: Opportunistic Unlicensed Reuse of Government Spectrum,* 24 INT'L J. OF COMMC'NS L. & POL'Y 1067 (2009)

52 *Id.*

53 *Id.*

54 Tim Wu, Op-Ed., *OPEC 2.0*, N.Y. TIMES, July 30, 2008, § A, at 17.

55 *Id.*

56 DALE HATFIELD & PHIL WESIER, CATO INST., TOWARD PROPERTY RIGHTS IN SPECTRUM: THE DIFFICULT POLICY CHOICES AHEAD 4 (2006).

57 Sascha Meinrath & Victor W. Pickard, *Revitalizing the Public Airwaves: Opportunistic Unlicensed Reuse of Government Spectrum,* 24 INT'L J. OF COMMC'NS L. & POL'Y 1067 (2009)

58 NUECHERTERLEIN & WEISER, *supra* note 39, at 239.

59 ERIC A. HALL, INTERNET CORE PROTOCOLS: THE DEFINITIVE GUIDE 8 (2000).

Enclosures at the data link layer can make communication inoperable by "leap-frogging" into the functionality of other layers, differentiating between types of communication, and creating virtual circuits that can control or break end-to-end functionality. The third layer of the OSI model is the network layer and enables full network communication. In the TCP/IP framework of the Internet, the Internet Protocol comprises the network layer and provides the foundation for most end-to-end communications by bridging node-to-node communication of the data link layer and helping to maintain the quality of service requests of the transport layer.[60]

1. Internet Protocol Addresses

Internet Protocol is central to connecting devices over their physical networks and requires addresses to identify different devices like. Much like a telephone number rings a specific device or address, Internet protocol addresses routes data to specific destinations on a network or across networks.[61] There current dilemma is between two versions of the IP protocol: IPv4 and IPv6. Introduced in 1981, IPv4 uses a 32-bit address space and can support a maximum of 4.3 billion addresses (2^{32}),[62] a number once thought to be sufficient to support future devices. However, just ten years after its introduction, fears soon mounted about "address space exhaustion," or usage of all 4.3 billion addresses. These fears have come to fruition. While all IPv4 addresses have not been distributed, the IPv4 address space has been exhausted.[63] While work-arounds like network address translation ("NAT") help slow the rate of exhaustion, it will become increasingly difficult to add publicly addressable devices, websites, and destinations as the last IPv4 addresses are distributed.[64]

Version six of the IP protocol was developed to address this problem.[65] IPv6 contains 2^{128} addresses (about 3.4×10^{38}).[66] That number will sufficiently provide enough IP addresses to assign one to every atom on the surface of the Earth (and then do the same for 100 more Earths).[67] It is also enough to give

---

60 *Id.*

61 *Id.* at 10.

62 LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE 2 (MIT Press 2009) [hereinafter PROTOCOL POLITICS].

63 *See* Iljitsch van Beijnum, *River of IPv4 Addresses Officially Runs Dry*, ARS TECHNICA (Feb. 3, 2011, 9:15AM), http://arstechnica.com/tech-policy/news/2011/02/river-of-ipv4-addresses-officially-runs-dry.ars.

64 PROTOCOL POLITICS, *supra* note 62, at 156.

65 *See* Iljitsch van Beijnum, *Everything You Need to Know About IPv6*, ARS TECHNICA (Mar. 7, 2007, 9:10PM), http://arstechnica.com/hardware/news/2007/03/IPv6.ars

66 *Id.*

67 *See* Posting of Ivy Wigmore to IT Knowledge Exchange, http://itknowledgeexchange.techtarget.com/whatis/ipv6_address_how_many-is-that-in-

each of the 6.9 billion people alive today more IPs than ever existed in the entirety of IPv4 and still have hundred upon hundreds upon hundreds of billions of IPs left over.

Globally, IP address allocation has been primarily Americentric. In 2009 it was estimated North America currently had 32% of IPv4 addresses,[68] and at one point, Stanford University had more address allocations than China.[69] A similar trend may emerge for IPv6 distribution–73% of recent address allocations went to Europe and North America, compared to the 63% of IPv4 addresses allocated to the two continents as of 2009 despite only representing $1/5^{th}$ of the world's population and allocating a disproportionately small allocation to the fastest growing regions.[70] One would expect that, with a *de facto* unlimited supply, IPv6 addresses should cost next to nothing. Instead, a nearly identical pricing regime for IPv4 address space has been carried over into IPv6 address space[71]—creating a potential cost barrier to smaller networks or developing countries for a plentiful commodity. A quick review of the American Registry for Internet Numbers demonstrates that the fee schedule for IPv4 and IPv6 begins at a cost of $1250/year for a "X-small" allocation to $18,000/year for an "X-large" allocation:[72]

IPv4 ISP Annual Fees

Size Category	Fee (US Dollars)	Block Size
X-small	$1,250	smaller than /20
Small	$2,250	/20 to /19
Medium	$4,500	larger than /19, up to and including /16
Large	$9,000	larger than /16, up to and including /14
X-large	$18,000	larger than /14

numbers/ (Jan. 14, 2009, 7:26 AM).

68 PROTOCOL POLITICS, *supra* note 62, at 173.

69 *Id.* at 155.

70 *Id.* at 173.

71 *See Fee Schedule,* AM. REGISTRY FOR INTERNET NUMBERS, http://www.arin.net/fees/fee_schedule.html (last visited May 14, 2011). Though it should be noted that one does receive substantially more IPv6 IP addresses for the same price vis-à-vis IPv4 IP addresses, the main barrier for many new entrants and is often the cost, not the number of IP addresses.

72 *Id.* For an descriptions of IP block size, *see Understanding IP Addressing, Ripe* NETWORK COORDINATION CENTRE, http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing (last visited May 14, 2011).

IPv6 Annual Fees[73]

Size Category	Fee (US Dollars)	Block Size
X-small	$1,250	smaller than /40
Small	$2,250	/40 to /32
Medium	$4,500	/31 to /30
Large	$9,000	/29 to /27
X-large	$18,000	/26 to /22
XX-large	$36,000	/22 and larger

In the United States, the lack of national policy for transitioning to IPv6 creates uncertainty about how the distribution of remaining IPv4 addresses will take place.[74] IPv4 exhaustion may be creating a grey market for these increasingly valuable addresses, which will inevitably lead to a digital divide between those who can afford the addresses and those who cannot.[75]

Furthermore, because IPv6 and IPv4 cannot communicate directly with one-another, networks on legacy IPv4 networks will have to use IPv4 to IPv6 translation techniques to enable them to connect to IPv6-enabled providers.[76] Likewise, early adopters of IPv6 may find themselves having problems if their upstream provider is still using IPv4.[77] Finally, users of IPv4-only networks may find themselves unable to reach IPv6 destinations, further exacerbating the digital divide.[78] In essence, IP addresses become another way that dominant market players—those with control over key assets—can leverage control over higher layers of the OSI stack.

---

[73] To incentivize adoption of IPv6, the American Registry for Internet Numbers instituted fee waivers that pay for a diminishing amount of these fees year to year and phase out entirely in 2012. *Id.*

[74] While the Office of Management and Budget has pushed for federal networks to transition to IPv6, there has not been a domestic IPv6 policy. *See* OFFICE OF MGMT. & BUDGET (OMB), EXEC. OFFICE OF THE PRESIDENT, M-05-22, TRANSITION PLANNING FOR INTERNET PROTOCOL VERSION 6 (IPV6) (2005) (describing the OMB's transition attempts).

[75] Mel Beckman, *Beware the black market rising for IP addresses,* INFOWORLD (May 3, 2010), http://www.infoworld.com/d/networking/beware-the-black-market-rising-ip-addresses-729.

[76] *See* van Beijnum, *supra* note 65 ("Although designing a new protocol isn't exactly trivial, the hard part is getting it deployed. Having to put an entire new infrastructure in place or flipping a switch from "IPv4" to "IPv6" for the current Internet aren't feasible. To avoid these issues as much as possible, the IETF came up with a number of transition techniques.").

[77] *See* Iljitsch van Beijnum, *River of IPv4 Addresses Officially Runs Dry*, ARS TECHNICA (Feb. 3, 2011 9:15AM), http://arstechnica.com/tech-policy/news/2011/02/river-of-ipv4-addresses-officially-runs-dry.ars.

[78] *See IPv4 Deployment Frequently Asked Questions,* RIPE.NET, http://www.ripe.net/info/faq/IPv6-deployment.html (last visited May 14, 2011).

IP addresses can also be used to disrupt communications by enabling network administrators to censor particular content, specific users, or even entire regions of the Internet. IP addresses can be blocked individually or as blocks by a variety of entities—for example, schools or businesses can block access to certain Web sites or Web sites can block user access to content. Although IP address blocking can be used beneficially—such as to block spam—[79] the same means can also improperly inhibit legitimate communications. ISP blocking of IP addresses remains one of the greatest challenges.

Effects on users can be unintentional. For example, on December 22, 2004, Verizon started blocking e-mail sourced from IP addresses that originated from European ISPs.[80] Though it intended to identify and block spam, many of the blocked IP addresses were not sources of spam. Although the embargo was later identified to be a result of over-vigilant spam filters, the damage to communication was evident to users, resulting in a class action suit.[81] Verizon is not the only ISP to encounter problems in differentiating spam mail from legitimate mail. Two years earlier in October 2002, a similarly overly sensitive spam filter blocked a week's worth of incoming email for Earthlink subscribers.[82]

IP addresses can also be used to block access to certain websites by an ISP, or by a website to block access to certain users. In July 2009, AT&T blocked the imageboard website 4Chan, preventing any user on AT&Ts network from accessing the website.[83] Similarly, Wikipedia sometimes block users from editing its content,[84] and Ticketmaster uses IP addresses to identify and block bulk purchasing of tickets.[85] Left unchecked, IP blocking can have profound im-

---

[79] ALEXANDER R. GALLOWAY, PROTOCOL: HOW CONTROL EXISTS AFTER DECENTRALIZATION 119 (MIT Press 2004).

[80] John Gartner, *Verizon E-mail Embargo Enrages*, WIRED (Jan. 20, 2005), http://www.wired.com/techbiz/media/news/2005/01/66226.

[81] Nate Anderson, *Verizon proposes settlement for class action lawsuit*, ARS TECHNICA (Apr. 5, 2010, 11:10 AM), http://arstechnica.com/old/content/2006/04/6525.ars.

[82] Michelle Delio, *When Everything Was Spam to ISP*, WIRED (Nov. 11, 2002) http://www.wired.com/science/discoveries/news/2002/11/56235.

[83] Jacqui Cheng, *AT&T: 4chan block due to DDoS attack coming from 4chan IPs*, ARS TECHNICA (July 27, 2009, 12:47 PM), http://arstechnica.com/telecom/news/2009/07/att-4chan-block-due-to-ddos-attack-coming-from-4chan-ips.ars.

[84] *See Wikipedia Blocking Policy*, WIKIPEDIA, http://en.wikipedialorg/wiki/Blocking_policy (last visited May 14, 2011); *see also* Melissa McNamara, *Stephen Colbert Sparks Wiki War*, CBS NEWS (Aug. 9, 2006), http://www.cbsnews.com/stories/2006/08/08/blogophile/main1873436.shtml (reporting on when Wikipedia administrators blocked television personality Stephen Colbert and his fans from editing articles about elephants). *See also* Ryan Singel, *Wikipedia Bans Church of Scientology*, WIRED (May 29, 2009, 2:18 PM), http://www.wired.com/epicenter/2009/05/wikipedia-bans-church-of-scientology/.

[85] Kim Zetter, *Wiseguys Indicted in $25 Million Online Ticket Ring*, WIRED (Mar. 1, 2010, 12:57 PM), http://www.wired.com/threatlevel/tag/wiseguys/.

pacts on the ability to communicate freely.

2. IP Multimedia Subsystem ("IMS")

IMS is a still-evolving feature set for architecting wireline and wireless networks that has great potential to enclose portions of the next generation communications systems. Telecommunications firms have been particularly focused on deploying IMS in their wireless networks.[86] The Internet is a packet-switched network—information is broken into packets on one end and can travel independently over multiple pathways to be reassembled on the receiving end.[87] However, IMS can make communication resemble more of a circuit-switched network.[88] Like the days of copper-wire telephone, IMS allows a carrier to earmark specific channels for specific communications, thus creating the ability for bill differentiation among data types that are actually traversing the same network architecture. In other words, Internet traditionally had an application agnostic approach, allowing allow a user to send e-mail, use Skype, surf the web, and IM with friends for a single fee, wireless networks employ IMS to differentiate these services.

The low barriers to entry of the open Internet allows developers to innovate and create new ways to use bandwidth resources. However, quality of service implementations like IMS predefine the value of certain uses of network bandwidth and freeze prioritization for certain services and applications.[89] The existing application differentiated charges on cellular phone networks suggest a nefarious pricing regime: while residential broadband connectivity costs $0.01 per megabyte regardless of use, wireless voice costs $1.00 per megabyte of bandwidth, and text messages are extraordinarily priced at over $1,000 per megabyte.[90]

IMS can allow this pricing regime to continue even though changes should

---

[86] *See* Rich Karpinski, *Services, LET Help Renew IMS Push*, CONNECTED PLANET (Sept. 24, 2009), http://connectedplanetonline.com/service_delivery/news/services-lte-help-ims-push-0924/.

[87] *See* ERIC A. HALL, INTERNET CORE PROTOCOLS: THE DEFINITIVE GUIDE 14-17 (2000) (describing the Internet Protocol).

[88] John G. Waclawsky, *IMS: A Critique of the Grand Plan*, 35 BUS. COMMC'NS REV. 54, 55 (Oct. 2005).

[89] M. CHRIS RILEY & ROBB TOPOLSKI, FREE PRESS & NEW AMERICA FOUNDATION POLICY BRIEF THE HIDDEN HARMS OF APPLICATION BIAS 6 (Nov. 6, 2009), *available at* http://www.newamerica.net/publications/policy/the_hidden_harms_of_application_bias.

[90] *See* Andrew Odylzko *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets* 4-5 (Digital Tech. Center, Univ. of Minn., Jan. 17, 2009), *available at* http://www.dtc.umn.edu/~odlyzko/doc/net.neutrality.pdf; *see also* Andrew Odylzko, *Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation* 4, (Digital Tech. Center, Univ. of Minn., Aug. 2004), *available at* http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf.

allow greater end-user flexibility. While 3G cellular networks have separate channels for different types of network access to allow prioritization of voice and differentiated billing,[91] 4G networks are based on IP, allowing for end-to-end communication.[92] Eventually, voice will be operated using solely VoIP, creating the flattened network dynamics seen in wireline connectivity. In the name of managing scarce spectrum resources, wireless providers choose to exert centralized control over an end-to-end network, instead of upgrading their networks with additional capacity—a process that would make these prioritizations irrelevant and greatly benefit consumers. IMS will allow carriers to charge users multiple times by differentiating uses over the same network–once for a voice plan, a second time to surf the web or send e-mail, and a third time to send text messages to friends. As John Waclowski writes, "[w]ith IMS, you will never know if you are getting the advertised broadband capacity you think you are paying for. The actual bit rate will be a function of what IMS thinks you are doing."[93]

3. Media Access Controller

Every network interface controller such as wireless cards and Ethernet cards, has a unique identifier built into the device called a Media Access Controller ("MAC") address. MAC addresses, which are more static than IP addresses, are often used to identify devices on a network.[94]

Since they are unique identifiers, MAC addresses can be used by security systems (such as those built in to Wi-Fi routers) to deny access to a network.[95] For example, a user who purchases Internet connectivity in a hotel room on a laptop would not be able to transfer connectivity to a smart phone or tablet; the user would have to repurchase connectivity for each additional device. MAC addresses enable restrictive pricing schemes that create more opportunities to charge consumers for connectivity.

Network operators have experimented with exploitative pricing in the residential wireline connectivity realm, as well. ISPs have attempted to control the number of devices their users could connect to their network—much in the

---

[91] Gilles Bertrand, *The IP Multimedia Subsystem in Next Generation Networks*, 2 (May 30, 2007), http://www.rennes.enst-bretagne.fr/~gbertran/files/IMS_an_overview.pdf.

[92] Jose Vilches, *Everything You Need to Know About 4G Wireless Technology*, TECHSPOT (Apr. 29, 2010), http://www.techspot.com/guides/272-everything-about-4g/ ("Besides speed, several other guidelines have been traced for wireless communication standards to qualify as 4G. In a nutshell, they should...be based on an all-IP packet switched network.").

[93] *See* Waclawsky, *supra* note 88, at 55.

[94] NEWTON'S TELECOM DICTIONARY 574 (23d ed. 2007).

[95] *Tip: Enable and Configure MAC Address Filtering*, TECHNET MAGAZINE, http://technet.microsoft.com/en-us/magazine/ff521761.aspx (last visited May 14, 2011).

same way that AT&T did prior to the Carterfone decision—[96] by locking in a specific MAC address as the only authorized device allowed on the home connection.[97] This lead to the widespread use of "MAC spoofing"—a process whereby one can manually change the MAC address of one device to emulate another device's MAC address.[98] In the hotel example, a user who changes the MAC address of their second device to mirror the MAC address of the authorized would be able to connect additional devices to the network using the same account. Home users could spoof the MAC address of the computer that was registered with their ISP, enabling them to route around the barriers created by service providers to connect multiple devices through the router to their Internet uplink.

4. IMEI

Much like MAC addresses, cell phones also have unique identifiers embedded in their firmware. Each Subscriber Identity Module ("SIM") card has an International Mobile Equipment Identity ("IMEI") number. The IMEI authenticates a cellular device with a network and allows the device to communicate.[99] IMEIs can also function as tracking identifiers—a major concern for privacy. Mobile devices broadcast IMEIs to authenticate a device when connecting to a cell tower.[100] IMEIs expand the scope of who is able to track users beyond law enforcement officials and network operators. In fact, some stores have used cell signals to track a shopper's movement and patterns, enabling them to gather valuable information, such as which aisles they visited and how much time is spent in front of a display.[101] These types of surveillance are automatic, and make it difficult for users to know when they are being monitored or to know how to opt out. More recently, a German elected official sued for data retained by his cell phone carrier and found that Deutsche Telekom had

---

[96] *Carterfone Decision*, *supra* note 34, at 421 ("[AT&T] advised their subscribers that the Carterfone, when used in conjunction with the subscriber's telephone, is a prohibited interconnecting device").

[97] *No Internet with New Router, Computer, or Adapter: MAC Spoofing*, NETGEAR (Mar. 18, 2011, 3:33 PM), http://kb.netgear.com/app/answers/detail/a_id/1086/~/no-internet-with-new-router,-computer,-or-adapter%3A-mac-spoofing .

[98] Chad Perrin, *How to Spoof a MAC Address*, TECHREPUBLIC (Jan. 22, 2008, 1:28 PM), http://www.techrepublic.com/blog/security/how-to-spoof-a-mac-address/395.

[99] NEWTON'S TELECOM DICTIONARY 482 (23d ed. 2007).

[100] CHEN HUI ONG NELLY KASIM, SAJINDRA JAYASENA, LARRY RUDOLPH, TAT JEN CHAM, PROACTIVE DETECTION AND RECOVERY OF LOST MOBILE PHONES (2004), *available at* http://dspace.mit.edu/bitstream/handle/1721.1/7432/CS022.pdf?sequence=1.

[101] Jonathan Richards, *Shops track customers via mobile phone: Signals given off by phones allow shopping centres to monitor how long people stay and which stores they visit*, THE TIMES (May 16, 2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ece.

"recorded and saved his longitude and latitude coordinates more than 35,000 times."[102] Over time, these invasive actions can allow companies to build up remarkably detailed and valuable profiles of cell phone users. It is not far-fetched to imagine that sometime in the near future, these companies could partner with third parties to target advertisements directly to one's front door. Access to information private user data such tracking a mobile user's location not only raises privacy concerns but also represents a case of a carrier or other entity harvesting user data without the user consent or knowledge and gaining value from a customer beyond the transparent transaction of purchasing a communication's service.

5. Copyright Enforcement vs. Fair Use

Many efforts to stem the transfer of copyrighted material online take advantage of certain facets of the OSI model. Some countries have proposed or passed laws to terminate the Internet connection to a household if a user of that household's Internet connection transfers copyrighted material three times. France's legislation, in particular, has been on the forefront of blocking Internet access over copyright violations. Originally proposed in March of 2009, the law "Création et Internet" creates a new group, HADOPI, [103] to compile and maintain a blacklist of accused households. After a third accusation of infringing on copyright, a household is blacklisted and cut off from Internet access from any ISP for three months to a year.[104] After failing to gain support, a revised version of the bill was passed in September 2009, holding users responsible for any use on their network.[105] Ireland has followed with similar legisla-

---

[102] Noem Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1.

[103] HADOPI is the French agency charged with overseeing intellectual property. *See Hadopi – haute Autorité pour la diffusion des oeuvres et la protections des droits sur internet*, HADOPI, http://www.hadopi.fr.

[104] Nate Anderson, *French anti-P2P Law Toughest in the World*, ARS TECHNICA (Mar. 10, 2009, 11:25 PM), http://arstechnica.com/tech-policy/news/2009/03/french-anti-p2p-law-toughest-in-the-world.ars. *See also* Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la creation sur internet [Law 2009-669] of June 12, 2009 Promoting Dissemination and Protection of Creation on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANCAIS [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 12, 2009, Article L 331-29, *as amended by* CONSEIL CONSTITUTIONNEL [CC] CONSTITUTIONAL COURT] decision No. 2009-590DC. Oct. 22, 2009, 19292.

[105] Nate Anderson, *France Passes Harsh Anti-P2P Three-Strikes Law (Again)*, ARS TECHNICA (Sept. 15, 2009, 3:59 PM), http://arstechnica.com/tech-policy/news/2009/09/france-passes-harsh-anti-p2p-three-strikes-law-again.ars. *See also* Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la creation sur internet [Law 2009-669] of June 12, 2009 Promoting Dissemination and Protection of Creation on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANCAIS [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 12, 2009, Article L 331-29, *as amended by* CONSEIL CONSTITUTIONNEL [CC]

tion.[106] Only after vociferous objection was language recommending that all countries follow suit removed from the draft release of the Anti-Counterfeiting Trade Agreement released in April 2010.[107]

These legislative efforts shift considerable burden of proof to users rather than accusers. Violations of copyright can easily be unintentional, and consumers often do not fully understand convoluted intellectual property laws. Indeed, professionals apparently have difficulty as well. For example, like most government agencies HADOPI, the French agency charged with overseeing intellectual property created an emblem for the organization. However, in January 2010 a designer discovered that HADOPI, had violated copyright law by using a their font without permission.[108] The copyright infringement was later attributed to an unwitting mistake by an employee. As with many laws passed by legislators who do not understand the technologies involved, the actual detection mechanisms that underlie enforcement of these laws are left undefined. Such detection methods would almost certainly require some form of deep packet inspection, which is the technological equivalent within a packet-switched network to a wire tap on a circuit-based telephone system. The implementation of effective law enforcement mechanisms would require an invasive surveillance regime that would look at which devices are accessing specific materials and what the actual payload of individual packets contains. Privacy issues aside, such an enforcement mechanism can become quite problematic.

6. Tampering and Forging of Packets

The fact that the Internet is designed to be decentralized does not free it from direct manipulation. Analysis and control of substantive information flowing across networks is possible through a technique called deep packet inspection ("DPI"). In contrast to circuit-switched networks that have dedicated circuits, packet switched networks utilize discrete packets of information

---

CONSTITUTIONAL COURT] decision No. 2009-590DC. Oct. 22, 2009, 19292.

[106] Nate Anderson, *Major Labels Go Bragh? Irish Judge Allows 3 Strikes*, ARS TECHNICA (Apr. 19, 2010, 12:21 PM), http://arstechnica.com/tech-policy/news/2010/04/major-labels-go-bragh-as-irish-judge-allows-3-strikes.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss.

[107] *See Updated: New Zealand seeks to restrain ACTA,* COMPUTERWORLD (Mar. 2, 2010), http://computerworld.co.nz/news.nsf/news/leak-new-zealand-opposes-acta. *See generally* CONSOLIDATED TEXT PREPARED FOR PUBLIC RELEASE ANTI-COUNTERFEITING TRADE AGREEMENT (Apr. 2010), *available at* http://www.ustr.gov/webfm_send/1883.

[108] Cory Doctorow, *France's anti-piracy goon squad pirates the font in its logo*, BOINGBOING (Jan. 12, 2010, 10:22 PM), http://www.boingboing.net/2010/01/12/frances-anti-piracy.html.

that contain delivery information as well as substantive content.[109] In the same way that a postal employee can tamper with mail in transit, DPI enables ISPs to tamper with packets in transit through their networks. Unlike the strict laws against tampering with mail, however, there are no rules or regulations hold ISPs accountable for nefarious behavior.[110]

Tampering can also take the form of injecting falsified traffic into the network data stream. ISPs may terminate a selected application's communications by forging packets that trick end-users' computers into thinking that the connection has been interrupted. There was such an occurrence in 2007, when an engineer named Robb Topolski noticed that file transfers using the peer-to-peer software BitTorrent were not transferring properly. Topolski discovered that his ISP, Comcast Communications, was intercepting packets sent from his computer and injecting reset packets that caused his computer to believe that connections to BitTorrent servers had been aborted, causing the file transfer he was attempting to slow down or to be terminated entirely.[111] In essence, Comcast was pretending to be one party involved in the file transfer and terminating the communication, interrupting normal TCP/IP communication.[112] The Associated Press and the Electronic Frontier Foundation were able to duplicate Topolski's results. At the time, Comcast had not disclosed that it was engaging in this practice, and despite evidence implicating their network management practices, actually denied interfering with BitTorrent transfers at all. Eventually, Comcast settled a class action lawsuit for $16 million.[113]

A user's ability to define its Internet experience depends on the freedom to use the application of their choice. As the Comcast case highlights, an ISP does not need to have direct access to a user's computer to exercise de facto control

---

[109] ERIC A. HALL, INTERNET CORE PROTOCOLS: THE DEFINITIVE GUIDE 11 (2000).

[110] The Open Internet Order adopted December 23, 2010 by the FCC does not directly prohibit use of DPI. It only prohibits unreasonable network management practices. *In re* Preserving the Open Internet; Broadband Industry Practices, *Report and Order*, GN Docket No. 09-191, WC Docket No. 07-52, ¶ 82 (Dec. 23, 2010).

[111] *In re* Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices Petition of Free Press *et al.* for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management", *Memorandum Opinion and Order*, 23 F.C.C.R. 13,028, ¶ 9 (Aug. 1, 2008).

[112] *Id.* at ¶ 8.

[113] Jacqui Cheng, *Comcast settles P2P throttling class-action for $16 million*, ARS TECHNICA (Dec. 22, 2009, 3:22 PM), http://arstechnica.com/tech-policy/news/2009/12/comcast-throws-16-million-at-p2p-throttling-settlement.ars; Nate Anderson, *Just like Comcast? RCN accused of throttling P2P*, ARS TECHNICA (Apr. 20, 2010, 12:42 PM), http://arstechnica.com/tech-policy/news/2010/04/just-like-comcast-rcn-accused-of-throttling-p2p.ars .

over which applications customers can run. The surreptitious nature of this type of control effectively prohibits all but the most savvy users from knowing when their communications are at risk.

7. Blocking Video

Faster broadband speeds have increased the viability of the Internet to distribute video content, but online video content is not universally accessible. Some ISPs block content based on the location of the end-user, while others block content according to the source of the content. In essence, network owners are able to define what content users access, instead of the end-users themselves.

For example, blocked video content is commonplace on MLB.tv, Major League Baseball's (MLB) Web site, which offers subscription service to allow fans to watch "every out of market game" and advertises a total availability of 2,430 games.[114] However, the services stipulate that games are subject to local black outs "in each applicable Club's home television territory."[115] This is significant not just because games are blacked out based on geographic location, but because MLB.tv determines blackouts based upon users' IP addresses in order to identify the location of each Web user.[116]

Agreements between content providers and ISPs frequently govern user access to content. For example, ESPN3 offers a live video streaming service.[117] These services are touted as "free of charge" for users who receive service from a "participating high speed internet service provider."[118] DSLreports.com reports that these participating ISPs have paid ESPN for access to the content for their uses,[119] forcing customers to pay for a service even if they do not use

---

[114] Mark Newman, *MLB.TV is the ideal Gift for a Baseball Fan,* MLB.COM (Dec. 16, 2010, 10:00 AM), http://www.mlb.mlb.com/news/article.jsp?ymd=20101214&content_id=16320966&vkey=news_mlb&c_id=mlb; *see also MLB TV Demo Video,* MLB.COM, http://mlb.mlb.com/mlb/subscriptions/index.jsp?product=mlbtv&affiliateId=MLBTVREDIRECT (last visited May 14, 2011) (stating that viewers would have access to "every out of market game" and displaying an opening graphic showing the availability of 2,430 games, subject to blackout and local market rules).

[115] *See Watch Live Streaming Baseball Online with MLB.TV,* MLB.COM, http://mlb.mlb.com/mlb/subscriptions/index.jsp?product=mlbtv&affiliateId=MLBTVREDIRECT (last visited May 14, 2011).

[116] *See id.* (noting that "MLB.com live game blackouts are determined in part by IP address. MLB.com At Bat live game blackouts are determined using one or more reference points, such as GPS and software within your mobile device. The Zip Code search is offered for general reference only.").

[117] *ESPN Fact Sheet,* ESPN (Jan. 10, 2010), http://espnmediazone3.com/wpmu/.

[118] *See ESPN 3 FAQ,* ESPN, http://espn.go.com/broadband/espn360/faq#2 (last visited May 14, 2011).

[119] Karl Bode, *Small ISPs Revolt Against ESPN360 Model,* DSL REPORTS (Feb. 12,

it, want it, or even know of its existence. Broadcasters have also used a similar model to limit access to online content. When it aired the 2010 Winter Olympics, NBC limited access to online content to users accessing the Internet through ISPs that also have videos that included NBC content.[120] NBC also reportedly asked Canadian ISPs to block access from U.S. users so that Americans would have to watch programming during prime time hours, presumably so NBC could charge a premium for advertising on their network.[121]

Finally, it is important to note that proponents of content blocking and declarations go well beyond networks such as ESPN, NBC, and MLB. The single biggest purveyor of this technology is China,[122] which uses the same technologies to control access to content by its citizenry. While the rationale may be different,[123] the technical underpinnings of this form of digital feudalism, regardless of who perpetuates it, are the same.

C. Transport Layer Problems

The transport layer is responsible for quality control and reliability.[124] The transport layer is the transmission control protocol (TCP) component of a TCP/IP network and has been under attack by telecommunications companies striving to integrate "quality of service" techniques that would oversee how transport is controlled.[125]

Several incumbents have begun a campaign for a false dichotomy between speed and openness, arguing that capacity limitations, Quality of Service implementations, and network management requirements require a more closed approach at the transport layer.[126] Whereas incumbents obviously benefit from

---

2009), http://www.dslreports.com/shownews/100843; Karl Bode, *ESPN 360 ISP Model Spreads To HBO, Olympics*, DSL REPORTS (Feb. 17, 2010) http://www.dslreports.com/shownews/106949.

[120] *See Alex Weprin,* Zucker Defends NBCU's Online Strategy for Olympics, BROADCASTING & CABLE (Apr. 1, 2010, 10:32 PM), http://www.broadcastingcable.com/article/450958-Zucker_Defends_NBCU_s_Online_Strategy_for_Olympics.php (explaining NBC's 2010 Olympic content policy).

[121] Lisa Hoover, *Where Can I Watch the Olympics Online*, LIFEHACKER (Feb. 12 2010, 11:15AM), http://lifehacker.com/#!5469488/where-can-i-watch-the-olympics-online.

[122] *See How Censorship Works in China: A Brief Overview*, HUMAN RIGHTS WATCH (Aug. 2006), http://www.hrw.org/reports/2006/china0806/3.htm ("China's Internet regulations may be among the most extensive and restrictive in the world.").

[123] *Id.* (explaining that Chinese law censoring Internet content is based on the desire to control its citizenry morally and politically).

[124] Eric A. Hall, Internet Core Protocols: The Definitive Guide 8 (2000).

[125] ANDREW G.BLANK, TCP/IP FOUNDATIONS 1 (2004); *see also* NEWTON'S TELECOM DICTIONARY 1093 (25th ed. 2009).

[126] *See, e.g., In re* Preserving the Open Internet; Broadband Industry Practices, *Comments of AT&T Inc.*, GN Docket No. 09-191, WC Docket No. 07-52, at 37 (Jan. 14, 2010)

this dichotomy, the same cannot be said for the general public. The fact remains that openness, by eliminating barriers to innovation, facilitates packet flow, and upgrades paths, which in turn fosters higher speed networking.[127]

Cable network operators face challenges over the medium-term as they attempt to deal with severe architectural limitations and upgrade to DOCSIS 3.0.[128] On the other hand, Verizon and other fiber-heavy ISPs are in a good position to leverage their speed into *de-facto* monopolies, yet they have dramatically slowed their planned rollouts, ceasing expansion to new cities in 2010.[129] Speed alone does not lend itself to monopoly, but once speed becomes a salient differentiator among networks (and without structural separation to ensure that ISPs cannot leverage Layer 1 control to lock down everything else), this is an area that will necessitate close observation in coming years.

1. Port blocking

A port is a software construct at the Transport layer that applications utilize to streamline communication over protocols like TCP.[130] Much like boats or planes use the same gates when loading and offloading customers, applications often use specific ports for sending and receiving data packets.[131] When an ISP blocks a specific port, it blocks any application that specifies that port for communication.[132] Although technically savvy users can route around this problem using port-forwarding,[133] port blocking is often the equivalent of a

---

(available via FCC Electronic Comment Filing System)

[127] *See* VAN SCHEWICK, *supra* note 1, 383-387. *See also* Ashsih Shat et. al., *Thinking About Openness in the Telecommunications Policy Context* 12-13 (Thirty-First Telecomms. Policy Research Conference, Sept. 20, 2003), *available at* http://intel.si.umich.edu/tprc/papers/2003/244/openness2.pdf.

[128] Data Over Cable Service Interface Specification ("DOCSIS") is s standard that defines how to build a cable network to transport Internet traffic. *See Data Over Cable Service Interface Specifications: Physical Layer Specification*, CABLE TELEVISION LABORATORIES, INC. 1-4 (2010), http://www.cablelabs.com/specifications/CM-SP-PHYv3.0-I09-101008.pdf.

[129] Devindra Hardawar, *Verizon slows down expansion of its FiOS fiber network*, VENTURE BEAT (Mar. 26, 2010), http://www.venturebeat.com/2010/03/26/verizon-slows-down-expansion-of-its-fios-fiber-network/.

[130] *See* NEWTON'S TELECOM DICTIONARY 875 (25th ed. 2009).

[131] *See* Michael F. Morgan, *The Cathedral and the Bizarre: An Examination of the "Viral" Aspects of the GPL*, 27 J. MARSHALL J. COMPUTER & INFO. L. 349, 380 (2010).

[132] *See, e.g.*, David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, STAN. TECH. L. REV. 1, ¶ 41 (2005).

[133] *See Port Forwarding Definition from PC Magazine Encyclopedia*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=port+forwarding&i=49509,00.asp (last visited May 14, 2011). *See also* ELIZABETH D. ZWICKY, SIMON COOPER, & D. BRENT CHAPMAN, BUILDING INTERNET FIREWALLS, 505 (Deborah Russell & Nancy Crumpton, eds., 2d ed. 2000) (explaining that port forwarding "require[s] some knowledge of how the protocols work and the port numbers that are used.").

denial of service for the average user.

Perhaps the most notable incident of port-blocking occurred in early 2005, when VoIP provider Vonage reported that a local ISP blocked the use of its application and requested an investigation by the FCC. [134] On February 11, 2005, the FCC began an investigation into non-functionality of Vonage on Madison Internet service.[135] The FCC eventually found that Madison River Telephone Company LCC "was cutting off access to Vonage and other VoIP services by blocking certain IP ports."[136] Madison River Telephone Company was fined $15,000 and ordered to not "block ports used for VoIP applications or otherwise prevent customers from using VoIP applications."[137]

Port blocking can negatively impact numerous other applications as well. In 2004, Comcast began blocking port 25[138] to stop spam sent from so-called "zombie computers."[139] Although Comcast reported a 35% decrease in spam,[140] the blocking of port 25 made it difficult for individual users to send legitimate e-mail using their own e-mail servers. It remains unclear how much of the 35% in "spam" was actually legitimate e-mail traffic.[141]

Port blocking can also invade user privacy and mine personal information by intercepting plain text, or limits what a user can accomplish with an Internet connection. Telnet, an early protocol used to create virtual terminals, transmitted data, including passwords, in plain text. Secure Shell (SSH) has replaced Telnet in most instances and creates secure communication between two devices. By creating a shell to encrypt data bits, communication can be resistant to deep packet inspection or snooping of malicious hackers or those seeking to look at what content you are transmitting or receiving. Default operation of SSH requires Port 22.[142] When this port is blocked, individuals lose the ability

---

[134] Stephen Lawson, *Vonage Says ISP Blocked Its Calls: A broadband provider prevented customers from using its service, company says*, PC WORLD (Feb. 16, 2005, 8:00 AM), http://www.pcworld.com/article/119695/vonage_says_isp_blocked_its_calls.html.

[135] *In re* Madison River Commc'ns, LLC & Affiliated Companies, *Consent Decree*, DA Docket No. 05-543, at ¶ 3 (Mar. 3, 2005) [hereinafter Madison River Consent Decree], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf.

[136] *Madison River to Pay FCC $15,000 for Port Blocking*, V2M VISION2MOBILE (Mar. 7, 2005), http://www.vision2mobile.com/news/2005/03/madison-river-to-pay-fcc-15-000-for-port-blocking.aspx.

[137] *See* Madison River Consent Decree, *supra* note 135, ¶ 5.

[138] Port 25 is used for SMTP (Simple Mail Transfer Protocol), the protocol used to send outgoing email from an email client such as Mozilla Thunderbird or Microsoft Outlook. *Port Numbers)*, IANA.ORG, http://www.iana.org/assignments/port-numbers (last visited May 14, 2011).

[139] Jim Hu, *Comcast takes hard line against spam*, CNET (June 10, 2004, 12:56 PM), http://news.cnet.com/2100-1038_3-5230615.html.

[140] *Id.*

[141] *See Port 25 Block – Can't Send Mail via Non-SBC Servers,* DSL REPORTS (Sept. 13, 2010, 4:30 PM), http://www.dslreports.com/faq/12321.

[142] Jaikumar Vijayan, *Novell Server Was Used to Look for Vulnerable Ports on Other*

to direct traffic to different places, conduct point-to-point tunneling, or maintain their security over the Internet. Thus, port blocking had directly infringed on users right to privacy. Blocking ports can also block end-user functionality. For example, Hypertext Transfer Protocol ("HTTP"), a vital protocol for displaying WebPages, can be blocked by blocking port 80, and limit the ability for an individual to run a webhosting server in their own home.

Ports are vital channels of communication for applications and servers. While interfering with ports can at times be used for beneficial purposes, such as preventing a denial of service attack or controlling spam, these restrictions hinder normal operation of the Transport layer and can lead to the development of more advanced malicious code.[143] Since many programmers know how to port forward who are able to route around the problem,[144] network operators end up punishing users, preventing them from using legitimate services and applications instead of those who engage in illegitimate actions. Furthermore, ISPs often block various ports without disclosure or advanced notice,[145] leaving consumers wondering why applications do not function as prescribed and unable to trust an application to work when needed.

D. Session Layer Problems

The Session layer manages the communication between computers and/or devices. A session is a single connection, or transfer of packets, between connected NICs.[146] While a user who operates a web browser may only need one session to download a webpage, the increasing complexity of today's Web pages often necessitates multiple connections, or sessions.[147] Furthermore, by running multiple sessions in parallel, one can greatly increase the page load

---

Computers, COMPUTERWORLD (Oct. 3, 2005, 12:00 PM), http://www.computerworld.com/s/article/105120/Novell_Server_Was_Used_to_Look_for_Vulnerable_Ports_on_Other_Computers_Worldwide.

[143] Kevin Werbach, *Only Connect*, 22 BERKELEY TECH L.J. 1233, 1280 (2007).

[144] *See also* ELIZABETH D. ZWICKY, SIMON COOPER, & D. BRENT CHAPMAN, BUILDING INTERNET FIREWALLS 505 (Deborah Russell & Nancy Crumpton, eds., 2d ed. 2000) (explaining that port forwarding "require[s] some knowledge of how the protocols work and the port numbers that are used.").

[145] *See, e.g., Comcast Blocking TCP Port 22 Inbound – Comcast Help and Support Forums*, Comcast.com, http://forums.comcast.com/t5/Connectivity-and-Modem-Help/Comcast-blocking-TCP-Port-22-inbound/td-p/783356 (last visited May 14, 2011).

[146] Paul Simoneau, *The OSI Model: Understanding The Seven Layers of Computer Networks*, GLOBALKNOWLEDGE.COM, 4, 7 (2006), http://www.crswann.com/4-Misc/WP_Simoneau_OSIModel.pdf.

[147] Mozilla Firefox 3, for example, allowed the user a default maximum of 6 simultaneous sessions connection with webservers, compared with the previous limit of 2. https://developer.mozilla.org/en/xmlhttprequest. This limit can be changed by the user: https://developer.mozilla.org/en/Mozilla_Networking_Preferences.

speed.[148] Multiple sessions also permits multi-tasking, by allowing multiple connections to webserver to simultaneous load different elements such as load a streaming video, send an email, an even loading multiple pages all at once. Session number limitations can dramatically impact how applications can engage with the Internet, the functionality of those applications, and an end-user's experience of those services and applications.

1. Session Limits

Beginning in 2005, and widely deployed in 2007, Comcast began monitoring the number of open sessions of specific applications in a region.[149] Using switching equipment from Sandvine, the PTS 8210,[150] Comcast was able to "identify unidirectional P2P uploads" of predefined protocols, such as Ares, BitTorrent, eDonkey, FastTrack, and Gnutella.[151] The Sandvine PTS 8210 is capable of inspecting packet header information through stateful packet inspection ("SPI")[152] and, as described in a filing to the FCC regarding the practice: "Comcast established thresholds for the number of simultaneous unidirectional uploads that can be initiated for each of the managed protocols in any given geographic area."[153] When the thresholds were reached, Comcast began terminating communication of the applications such as BitTorrent.

Comcast confounded the problem by creating thresholds for blocks of users in specific geographic areas.[154] Thus, so-called "overuse" of a specific application by one user can detrimentally impact legitimate use of that same application by another user in the neighborhood. For example, when Comcast found BitTorrent sessions that exceeded the Uni Threshold of 8 among a block of users, their network management systems blocked additional functionality.[155] A knowledgeable user can circumvent SPI by directly connecting to a device

---

[148] Faster Fox, for example, is an extension for Mozilla Firefox allowing the user to control the number of simultaneous connections to decrease the load time of websites. *Faster Fox,* http://fasterfox.mozdev.org/screenshots.html

[149] Letter from Kathryn A. Zachem, Vice President, Regulatory Affairs, Comcast Corp., to Marlene H. Dortch, Sec'y, Fed. Commc'ns Comm'n, File No. EB-08-IH-1518, WC Docket No. 07-52, Attachment A, at 5 (Sept. 19, 2008)[hereinafter Comcast Network Management Practices], *available at* http://downloads.comcast.net/docs/Attachment_A_Current_Practices.pdf.

[150] Sandvine PTS 8210 is widely deployed by providers to implement network management techniques. *See Sandvine Policy Traffic Switch 8210,* http://www.sandvine.com/downloads/documents/PTS8210_Datasheet.pdf (last visited May 14, 2011) (detailing product details and specifications).

[151] *Id.* at 7.

[152] *Id.*

[153] *Id.* at 4.

[154] *Id.*

[155] *See* Comcast Network Management Practices, *supra* note 149, at 10.

by secure tunneling, creating direct connection between two end-points and a technique Topolksi used to discover that its network provider blocked BitTorrent.[156] However, Comcast implemented thresholds that are beyond any users ability to control—because a single user in a network cannot prevent another user from running the application of their choice. Comcast created a limit on the use of a specific application independent of the actual capabilities of the network and engaged in a collective reprisal against an entire geographic area when it identified overuse. When these practices were discovered, Comcast provided false information to consumers and the media, stating that traffic was not being blocked, only "delayed" (the equivalent logic of stating that hanging up the phone on someone does not terminate the call, only delays it).[157] As the Comcast example illustrates, the ability for network providers to limit sessions negatively impacts a user's ability to control their communication over a network.

E. Presentation Layer Problems

The presentation layer creates the framework for displaying information in the application layer. Examples include protocols for the display of text, such as American Standard Code for Information Interchange ("ASCII"). Presentation layer components can also include encryption and compression.[158]

1.ASCII & Mime -- Websurfing & Email

ASCII is a character-encoding scheme that serves as the foundation for turning bits to text. Many character sets are based on ASCII,[159] but the code is intrinsically Americentric. Applications that utilize ASCII as the character-encoding scheme cannot use non-Latin languages.[160] This became particularly problematic with domain name addresses, in which every URL must display in ASCII leaving entire language groups unable to build URLs in their native tongues.[161]

---

[156] Daniel Roth, *The Dark Lord of Broadband Tries to Fix Comcast's Image*, WIRED (Jan. 19, 2009), http://www.wired.com/techbiz/people/magazine/17-02/mf_brianroberts.

[157] Brad Stone, *Comcast: We're Delaying, Not Blocking, BitTorrent Traffic*, N.Y. TIMES BITS BLOG (Oct. 22, 2007, 9:41 PM), http://bits.blogs.nytimes.com/2007/10/22/comcast-were-delaying-not-blocking-bittorrent-traffic/.

[158] VINT CERF, ASCII FORMAT FOR NETWORK INTERCHANGE, NETWORK WORKING GROUP. (Oct16, 1969).

[159] Many character sets are based on ascii such as UTF-8 and Unicode.

[160] *See* ASCII character table. Vint Cerf 1969, *supra* note 158.

[161] *Id.*

On November 16, 2009, the International Corporation for Assigned Names and Numbers ("ICANN"),[162] the body that coordinates naming schemes for the Internet, launched the IDN ccTLD Fast Track Process, the first step to including Internationalized Domain Names ("IDNs").[163] IDNs, domain names and extensions using non-Latin characters, would enable domain names could include non-Western languages for the first time.[164] Although this is a dramatic step forward, IDNs do not include all languages. Arabic, Chinese, Greek, and Japanese are among the ten additional languages added thus far;[165] but additional languages must be individually added through a request process.[166]

Multipurpose Internet Media Extension ("MIME") is a standard for formatting emails and providing support for body and headers in different character sets and attachments.[167] Data included in a MIME header defines the type of content in the email, if the message includes multiple parts, or if the data is encrypted. Like ASCII, the application function of MIME must be included in the MIME protocol. Defining the acceptable language of emails, if a character or character set is excluded, it functionally does not exist, affecting both addresses and email content. Thus, MIME created an electronic communications medium where certain languages can simply not be used to send e-mail to recipients.

The presentation layer is essential for translating machine-readable data in a user compatible form. However, limitations or restrictions at the presentation can define what languages are permissible and create barriers to users.

F. Application Layer Problems

The application layer bridges the presentation of data with the end-user. Providing the foundation for software, application layer elements include hypertext transfer protocol (HTTP) and file transfer protocol (FTP). Enclosure to

---

[162] *See International Corporation for Assigned Names and Numbers*, ICANN, http://www.icann.org.

[163] *See IDN ccTLD Fast Track Process,* ICANN, http://www.icann.org/en/topics/idn (last visited May 14, 2011).

[164] Jacqui Cheng, *Say hello to .* ﷺ *as domain names go truly global*, ARS TECHNICA (Oct. 30, 2009, 2:18 PM), http://arstechnica.com/web/news/2009/10/domain-extensions-go-global-goodbye-com-welcome.ars.

[165] *See* INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS, IDNS: INTERNATIONALIZED DOMAIN NAMES 3 (2009), *available at* http://www.icann.org/en/topics/idn/factsheet-idn-program-05jun09.pdf.

[166] *See The IDN ccTLD Fast Track Process is Open, ,* ICANN INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS, http://www.icann.org/en/topics/idn/fast-track/ (last visited May 14, 2011) (noting that the current number of received fast track requests is 33, representing 22 languages).

[167] *See* J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker, *RFC 1426, SMTP Service Extension for 8bit-MIMEtransport* (Feb. 1993), http://tools.ietf.org/html/rfc1426.

the application layer can cripple applications and communication.

1.DNS Hijacking

The Domain Name System Protocol ("DNS protocol") is the translation of IP addresses to text.[168] The protocol creates a system for more easily recognizable web addresses, allowing users to enter a web address such as www.newamerica.net, instead of the IP address 69.174.51.225. The web address then matches to an IP address run by, in this example, Mzima Networks and the New America Foundation's web server. If the query is resolved by a NXDomain response, the user is directed to the website. If a domain name does not exist, is not associated with an IP address, such as misspellings like www.newamerca.net, a HTTP gives a 404 error indicating that the webpage or server does not exist. Applications layer responses can interpret this error to the user through messages. For example, Firefox displays a message that instructs users to "[c]heck the address for typing errors such as [ww.example.com] instead of [www.example.com]."

Some ISPs have began implemented services where a server synthesizes an NXDomain response if a DNS query is not resolved, redirecting traffic rather than transmitting the error protocol to the application. In 2007, Cox Communications began experimenting with DNS redirection.[169] In June 2007, Verizon began trials under their Web Search Service,[170] and Comcast began trials in July 2009 for their Domain Name Helper service, redirecting mistyped URLs to an advertisement heavy website with a search function.[171] This service was rolled out nationally in August 2009.[172] Cox, Earthlink and Charter have all used redirection as well.[173] In a preliminary report on DNS modification, the ICANN Security and Stability Committee noted: "any party involved in the

---

[168] *See* RAMESH BANGIA, DICTIONARY OF INFORMATION TECHNOLOGY 177-178 (2010) (describing the domain name system).

[169] Karl Bode, *Cox Tests DNS Redirection Though they provide unimpacted DNS Servers*, BROADBAND DSL REPORTS (May 19, 2007) http://www.dslreports.com/shownews/83929.

[170] Karl Bode, *Verizon DNS Redirection the latest ISP to profit off your butterfingers*, BROADBAND DSL REPORTS (June 20, 2007), http://www.dslreports.com/shownews/Verizon-DNS-Redirection-85063.

[171] Chris Griffiths, *Domain Helper Service: Here to Help You, Comcast Voices*, COMCAST VOICES (July 9, 2009), http://blog.comcast.com/2009/07/domain-helper-service-here-to-help-you.html.

[172] *Id. See* Chris Griffiths, *Domain Helper National Rollout Begins*, COMCAST VOICES (Aug. 4, 2009), http://blog.comcast.com/2009/08/domain-helper-national-rollout-begins.html.

[173] Karl Bode, *Verizon DNS Redirection 'Service' Spreads*, BROADBAND DSL REPORTS (Nov. 5, 2007), http://www.dslreports.com/shownews/Verizon-DNS-Redirection-Service-Spreads-89137.

resolution process can perform NXDOMAIN redirection for *every* name which it determines or is notified does not exist, regardless of whether or not an authoritative server gives an NXDOMAIN."[174]

DNS redirection can be a profitable endeavor whereby enclosure of traditional application layer functionality and neutral error messages can generate significant revenue. Often, web users would need to opt out of these redirection "services" if they want to actually know what errors they are actually receiving when a web page will not load. According to DSLreports.com, DNS redirection can boost revenue for ISPs by $5 per month for every user.[175] ICANN Senior Security Technologist Dave Piscitello has expanded the possibility for redirection, suggesting that it could be used for other IP-based applications such as redirecting e-mail or a VoIP phone call to a wrong number.[176] One example of a more invasive redirect occurred in April 2010 when users found that Windstream was redirecting their searches using the Google search bar to a competitor's search service,[177] though Windstream called this redirection accidental and changed it the next day, it demonstrates how easily one could hijack traffic to send it to another site.[178] For example, an ISP could redirect all traffic from Ford.com to Chevy.com or all traffic to McDonalds.com to BurgerKing.com. The ICANN board has banned the practice of redirection for new top level domains, however, as of this writing, ISPs such as Verizon and Comcast continue redirecting mistyped domains to their own services.[179]

2.H.264 and the Future of Online Video

As another example, the pooling of licenses for the H.264 codec is standardizing not only the technology, but the terms by which the technology itself can be used—thus already impacting the trajectory of innovation for next-

---

[174] ICANN SECURITY AND STABILITY ADVISORY COMMITTEE, SAC 032 PRELIMINARY REPORT ON DNS RESPONSE MODIFICATION 6, (June 2008), *available at* http://www.icann.org/en/committees/security/sac032.pdf.

[175] Karl Bode, *ICANN Slams DNS Redirection*, BROADBAND DSL REPORTS, (Nov. 25, 2009), http://www.dslreports.com/shownews/ICANN-Slams-DNS-Redirection-105651.

[176] Internet Corp. for Assigned Names and Numbers, *ICANN Start*, Episode 1: Redirection and Wildcarding (Mar. 2010), *transcript available at* http://www.icann.org/en/learning/transcript-icann-start-01-22mar10-en.pdf.

[177] Karl Bode, *Windstream Hijacking Firefox Google Toolbar Results*, BROADBAND DSL REPORTS (Apr. 5, 2010), http://www.dslreports.com/shownews/107744.

[178] Karl Bode, *Windstream Gives (Sort Of) Explanation For Google Search Hijack*, BROADBAND DSL REPORTS (Apr. 9, 2010), http://www.dslreports.com/shownews/107828.

[179] ICANN first "condemned" redirection in their 2009 Explanatory Memorandum. ICANN NEW GTLD PROGRAM EXPLANATORY MEMORANDUM 2 *et seq.* (Nov. 24, 2009); *See* Karl Bode, *ICANN Slams DNS Redirection*, BROADBAND DSL Reports (Nov. 25, 2009), http://www.dslreports.com/shownews/ICANN-Slams-DNS-Redirection-105651 (describing how the ICANN "condemned" redirection).

generation video services. The rising prevalence of online video has drawn attention to its dependency on third-party applications, such as Adobe Flash or Microsoft Silverlight.[180] The latest standards for hypertext markup language ("HTML") include new tags for making video support native, allowing users to view online video without external plugins. However, although the Internet is predicated on open standards one video standard included in HTML5 is the H.264 codec, a proprietary standard owned by the MPEG LA group.[181] With licenses held by Microsoft, Apple and others,[182] this codec builds privately owned, and potentially very expensive, standard into the Internet.

Video codecs are needed for encoders and decoders, such as video software, browsers, or video capable recording devices like digital cameras, or for content providers, such YouTube or over-the-air-television.[183] However, because H.264 is privately owned producers of software, browsers, or video recording devices will potentially have to pay to include the video standard. The availability of no-cost H.264 licenses were set to expire at the end of 2010, but MPEG LA in February 2010 announced an extension for no-cost licenses for "Internet Video that is free to end users (known as Internet Broadcast AVC Video)" through 2015.[184] This postpones the requirement that Vimeo or YouTube pay license fees for free video, but requires software developers to pay tribute in order to be compatible with online video. It remains to be seen what will happen in 2015, once the standard is more thoroughly embedded in multiple products.

The H.264 codec and its inclusion in HTML 5 has the potential to create a new bottleneck that captures a growing amount of online video traffic and could be utilized as a toll booth to create new "billable moments" for using these services. H.264 is quickly becoming the standard for online video. As of

---

[180] Adobe Flash and Microsoft are two existing plugins for displaying online video content. *See, e.g., Adobe Flash*, ADOBE, http://www.adobe.com/products/flashplayer/; *Microsoft Silverlight*, MICROSOFT, http://www.microsoft.com/silverlight.

[181] For more about MPEG LA, the patent pool behind H.264 and other MPEG standards, *see MPEGLA – The Standard for Standards*, MPEG LA, LLC, http://www.mpegla.com/main/default.aspx.

[182] *See AVC/H.264 Licensors*, MPEG LA, LLC, http://www.mpegla.com/main/programs/AVC/Pages/Licensors.aspx (last visited May 14, 2011) (naming Apple, Cisco, Microsoft, Microsoft and Sony among the number of licensors of H.264).

[183] *See generally* MPEG LA, SUMMARY OF AVC/H.264 LICENSE TERMS, *available at* http://www.mpegla.com/main/programs/avc/Documents/AVC_TermsSummary.pdf (last visited May 14, 2011).

[184] Press Release, Corrected Version of February 2, 2010 News Release Titled "MPEG LA's AVC License Will Continue Not to Charge Royalties for Internet Video that is Free to End Users" (Feb. 2, 2010), *available at* http://www.mpegla.com/Lists/MPEG%20LA%20News%20List/Attachments/226/n-10-02-02.pdf.

May 1, 2010, an estimated 66% of video content online is available through the H.264 codec, with the majority push coming from YouTube.[185] Constraining video to a particular license scheme is very troubling. Mozilla, for example, would need to pay a reported $5 million license fee in order to play H.264 encoded video on its Firefox web browser.[186] The license terms for H.264 could also be extended to devices like cameras and video game consoles as well as software, where this function is currently available for free.[187]

IV. THE NEED FOR OPEN TECHNOLOGY

At its heart, one of the most significant barriers to reform comes down to the differences between *closed* and *open* technologies. These notions often bring to mind issues related to open source and proprietary software (e.g., Linux versus Windows), but the distinction is more encompassing. Stolterman defines the important attributes as follows:

> A *closed technology* is one that does not allow the user to change anything after it has been designed and manufactured. The structure, functionality and appearance of the art[i]fact are permanent. . . . The technology is a relatively stable variable in social settings . . . . An *open technology* allows the user to continue changing the technology's specific characteristics, and to adjust, add/or change its functionality. When it comes to an open technology, changes in functionality pose a question not only of change in the way the existing functionality is used or understood but also of a real change in the art[i]fact's internal manifestation.[188]

The Internet was conceived and remains an open and designable technology. One can "add, embed, contain or surround the art[i]fact with other technology in a way that radically changes it."[189] This aspect has contributed to the successes of "Web 2.0" applications. However, actions such as Comcast blocking BitTorrent communications, the blocking of pro-choice text messaging by Ver-

---

[185] YouTube is estimated to account for 40% of all online video content. *See* Erick Schonfeld, *H.264 Already Won—Makes Up 66 Percent Of Web Videos*, TECHCRUNCH (May 1, 2010), http://techcrunch.com/2010/05/01/h-264-66-percent-web-video/.

[186] Stephen Shankland, *Mozilla takes on YouTube video choice,* CNET (Jan. 22, 2011, 2:16 PM), http://news.cnet.com/8301-30685_3-10440430-264.html.

[187] The license for H.264 used in digital cameras such as the Canon 5D or videos edited in Final Cut Pro only allows non-commercial use. *See* EOS 5D Mark II Instruction Manual 241 (2010), *available at* http://gdlp01.c-wss.com/gds/6/0300001676/02/eos5dmkii-im3-en.zip; *Apple Inc. Final Cut Studio Software License Agreement,* at 3, *available at* http://images.apple.com/legal/sla/docs/finalcutstudio2.pdf (last visited May 14, 2011).

[188] Erik Stolterman, *Creating community in conspiracy with the enemy, in* COMMUNITY INFORMATICS: SHAPING COMPUTER-MEDIATED SOCIAL RELATIONS 43, 45 (Leigh, Keeble & Brian D. Loader ed. 2001).

[189] *Id.*

izon, and the editing of a live Pearl Jam's concert by AT&T all attack this open framework.[190]

While corporations promise not to engage in such practices,[191] these "gentlemen's agreements" do nothing to prevent anti-competitive, anti-free speech, and anti-democratic actions from being repeated in the future. Unfortunately, by abdicating their responsibility to prevent this sort of corporate malfeasance, the FCC and other regulatory agencies are all but guaranteeing that these behaviors will continue.[192] As we have shown, discriminatory practices are being built into the very foundations of next-generation network infrastructure.

A. Limitations on Today's Closed Networks

As the wireless industry aptly demonstrates, the convergence of networks and devices threaten user freedom. Many cellular phones are released with exclusivity agreements and carriers often restrict the functionality of the phones. For example, when Verizon introduced the Motorola V710 – the carrier's first phone with Bluetooth functionality – [193] it removed the ability to transfer files over Bluetooth,[194] forcing customers who wanted to do so to buy another accessory or pay for additional services. The Motorola Razr was one of the most

---

[190] *See* Gil Kaufman, *AT&T Admits It Edited Webcasts Before Pearl Jam's*, MTV NEWS (Aug.13, 2007, 3:31 PM), http://www.mtv.com/news/articles/1566946/20070813/pearl_jam.jhtml; Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, N.Y. TIMES, Sept. 27, 2007, at A1.

[191] AT&T has argued there is transparency "mandates would be both unnecessary and counterproductive in the wireless context" suggesting competition is sufficient. *See In re* Preserving the Open Internet Broadband Industry Practices, *Comments of AT&T, Inc.*, GN Docket No. 09-191, WC Docket No. 07-52 (Oct. 12, 2010), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7020916485. Google and Verizon, one of the largest Internet companies and one of the largest ISPs, offered a proposal of agreeable terms that were largely incorporated by the FCC for their Open Internet Rules, such as the general exclusion of wireless from meaningful consumer protections. *Google Public Policy Blog: A Joint Policy Proposal for an Open Internet*, GOOGLE (Aug. 9, 2010, 1:38 PM), http://googlepublicpolicy.blogspot.com/2010/08/joint-policy-proposal-for-open-internet.html

[192] For example, on November 5, 2010 the Benton Foundation, Center for Media Justice, Consumers Union and Public Knowledge urged the FCC to act on Open Internet rules rather than form market consensus. *See In re* Preserving the Open Internet Broadband Industry Practices, *Reply Comments of Benton Foundation, Center for Media Justice, Consumers Union, Media Access Project, New America Foundation, and Public Knowledge*, GN Docket No. 09-191, WC Docket No. 07-52 (Nov. 4, 2010), *available at* http://www.publicknowledge.org/files/docs/PIC_Wireless_reply_comments.pdf.

[193] Carmen Nobel, *Verizon to Launch Its First Bluetooth Phone*, EWEEK (July 26, 2004), http://www.eweek.com/c/a/Mobile-and-Wireless/Verizon-to-Launch-Its-First-Bluetooth-Phone/.

[194] Sascha Segan, *Motorola V710*, PCMAG (Aug. 26, 2004), http://www.pcmag.com/article2/0,2817,1639784,00.asp.

popular phones of the past decade, shipping 50 million units by July 2006,[195] yet different networks offered different models. Essentially carriers competed based on device not network capabilities.

The problems with this approach are best epitomized by the 2007 deal between Apple and AT&T, in which Apple made it's iPhone available to only AT&T's network, even though it could be used on any cellular network.[196] Likewise, AT&T only allows certain services and applications to run on the iPhone, even though the iPhone could run many additional programs that would be useful for end users. Innovative iPhone owners and entrepreneurs quickly found ways to unlock their device and install a growing option of aftermarket applications, but the business practice of "exclusive deals" is anti-competitive and results in extra work and costs are borne by the end-user. Although Apple released an application store in July 2008, it continues to keep tight control over what types of applications are available in the store. For example, Apple rejected some applications, such as Google Voice, because they "duplicate features that come with the phone."[197] Others were limited in the features they could offer. Thus, while Apple allowed Major League Baseball's application to stream video over 3G wireless, it limited streaming on Skype to Wi-Fi. Apple only announced in 2010 that it would allow VoIP applications over 3G networks into the iTunes App Store.[198] However, Apple has gone so far as to dictate in the iPhone Developer Program License Agreement that only certain programming techniques are allowed on their device and that "applications that link to Documented APIs through an intermediary translation or compatibility layer or tool are prohibited."[199] Apple rescinded this policy fol-

---

[195] *See* Press Release, Motorola Media Center, Motorola Ships 50 Millionth MOTORAZR (July 18, 2006) (*available at* http://www.motorola.com/mediacenter/news/detail.jsp?globalObjectId=7031_6980_23).

[196] *See* Barb Dybwad, *AT&T has iPhone exclusivity until 2012,* CNN TECH (May 11, 2010), http://articles.cnn.com/2010-05-11/tech/iphone.att.2012.mashable_1_apple-and-at-t-iphone-app-store?_s=PM:TECH (announcing the exclusivity deal between AT&T and Apple for their iPhone service). Although Verizon announced they would begin carrying the iPhone 4 in February 2010, current AT&T customers would incur an early termination fee of up to $325. The earliest an iPhone 4 customer on AT&T could switch to an alternative carrier without this switching cost would be summer 2012, nearly 18 months after an alternative was announced. *See Early Termination Fees*, AT&T WIRELESS, http://www.wireless.att.com/learn/articles-resources/early-term-fees.jsp (last visited May 14, 2011).

[197] Jason Kincaid, *Apple Is Growing Rotten To The Core: Official Google Voice App Blocked From App Store*, TECHCRUNCH (July 27, 2009), http://techcrunch.com/2009/07/27/apple-is-growing-rotten-to-the-core-and-its-likely-atts-fault/.

[198] Stacey Higginbotham, *Apple Brings 3G VoIP to the iPhone*, GIGAOM (Jan. 28, 2010, 11:35 AM), http://gigaom.com/2010/01/28/apple-brings-3g-voip-to-the-iphone/.

[199] Brian X. Chen, *Adobe Apps: Easier to Pass Through the 'i' of a Needle?*, WIRED (Apr. 8, 2010, 8:12 PM), http://www.wired.com/gadgetlab/2010/04/iphone-developer-

lowing an antitrust investigation by the European Union.[200] Carriers and handset manufacturers have collaborated to prevent the "jailbreaking" of mobile devices by keeping some software components in read-only memory or designing devices that automatically deactivate if unauthorized software is detected.[201] In contrast, the benefits of open architectures are clear:

An open architecture means fewer technological restrictions and, thus, the ability to explore more options. In an open architecture, there is no list of elements and protocols. Both are allowed to grow and change in response to changing needs and technology innovation. With an open architecture you are not making bets on a specific direction the technology will take in the future. You are not tied to a specific design or a particular vendor or consortium roadmap, so you can evaluate and select the best solution from a broad and energetic competitive field. Competition facilitates innovation and reduces equipment and implementation costs.[202]

The costs of closed architectures are particularly devastating because they impact almost every communications medium. Further, with the dissonance in openness between wireless and wireline networks, and the FCC's push for wireless to provide competition for wireline networks, the need for open networks has never been greater.[203] Although both Verizon and AT&T have declared their intention to run open networks, and the terms of 700 MHz spectrum auction included openness requirements on the new "C-Block" mobile phone band,[204] these details have not yet been clearly defined. While these approximations of openness are only baby steps from a fully proprietary infrastructure, it is encouraging that the trend is toward a more open, interoperable, and innovation-supporting network.

Most municipal and enterprise 802.11 (Wi-Fi/WiMAX) wireless networks

---

policy/.

[200] Press Release, European Union, Antitrust: Statement on Apple's iPhone policy changes (Sept. 25, 2010) (*available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1175&format=HTML&aged=0&language=EN&guiLanguage=en).

[201] Dan Meredith, Josh King, Sascha Meinrath, & James Losey, *Mobile Devices are Increasingly Locked Down and Controlled by the Carriers: How Cell Phone "Customization" Undermines End-Users by Redefining Ownership*, NEW AMERICA FOUNDATION (Oct. 13, 2010), http://oti.newamerica.net/blogposts/2010/mobile_devices_are_increasingly_locked_down_and_controlled_by_the_carriers-38418.

[202] John C. Waclawsky, *Closed Systems, Closed Architectures, & Closed Minds*, 5 BUS. COMMC'N REV. 61 (2004).

[203] *See* NATIONAL BROADBAND PLAN, *supra* note 7, at ch. 4.

[204] *In re* Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, *Second Report and Order*, 22 F.C.C.R. 15289, 15371, ¶ 224 (2007).

are entirely proprietary.[205] For example, a Motorola 802.11 system will not interoperate directly with a Tropos system, which will not interoperate directly with a Meru system, which will not interoperate directly with a Meraki system, etc. In fact, most consumers have no idea that the links they rely on to access Internet and Intranet services lock geographical areas into distinct path dependencies with specific vendors (and their specific capabilities and limitations). Many incorrectly assume the interoperability of applications, services, and communications, and the communities that people participate in are geographically dispersed, the immediate and long-term ramifications of this geospatial lock-in remain almost entirely unexplored. Closed technologies have the potential to constrain the positive potentials of the Internet if their widespread adoption stems more from an emphasis on corporate profits than maximizing wireless networks' public benefits. Today's battles over 802.11n Wi-Fi systems, WiMax, and 4G networking are all indicators of this ongoing tension.

Unlike the Internet, these wireless "last-mile" links can *disallow* users from extending the network (e.g., using bridges and routers), adding applications (e.g., VoIP, P2P, IRC, IM), interconnecting additional services (e.g., streaming servers, distributed file storage, local webhosting), or connecting directly with one another. The wireless medium resembles the era when AT&T's control over which devices could be connected to their network and which technologies would thus be developed. The long-term effects of wireless lock-in may be more detrimental than any policy previously witnessed in telecommunications history.

Thus far, regulatory bodies and decision-makers remain unwilling to address these fundamental concerns. While President Obama's first Chairman of the FCC, Julius Genachowski, had initially proposed to eliminate these discriminatory practices, the rules adopted by the FCC in late 2010 are limited and will not eliminate discrimination.[206] The first decade of the 21st century has drawn to a close and this inaction may have profound impacts on the development of feudalistic communications systems in the years to come. Emphasizing the enclosures that can be employed at different layers of communications technology illuminates the imperative of situating this debate within a larger vision of Internet openness. Today, we sit at a critical juncture for Internet policy and the opportunities that now abound for graceful reforms will soon disappear.

---

[205] *See* Vijay Chandramouli, *A Detailed Study on Wireless LAN Technologies* 5-6 (Dept. of Comp. Sci. and Engineering, Univ. of Texas at Arlington), *available at* http://www.uta.edu/oit/policy/ns/docs/wireless-paper-vijay.pdf.

[206] *See In re* Matter of Preserving the Open Internet broadband Industry Practices, *Report and Order*, 25 F.C.C.R. 17905, ¶¶ 39-43 (Dec. 21, 2010).

V. POLICY RECOMMENDATIONS FOR THE NEW CRITICAL JUNCTURE IN TELECOMMUNICATIONS

Many have analogized the Obama administration's treatment of the Internet to circumvent traditional media to Franklin Delano Roosevelt's (FDR) use of radio during his fireside chats.[207] However, many forget the more cautionary tale that this historical parallel exemplifies: FDR failed to seize the initiative to set the new media of broadcasting on a democratic course when he had a chance. As a result, the broadcast media became not only largely commercialized, but also largely inoculated against public interest regulation, never reaching its full democratic potential.[208] To avoid a similar fate, we suggest a list of policy recommendations to steer our new digital potentials toward more democratic ends.[209]

A. Physical Layer Solutions

First, we recommend that the FCC overturn its decision following the *Brand X* Supreme Court case[210] and restore common carriage provisions to all Internet service providers. Common carriage ensures that network operators lease their lines to all potential market players at wholesale market rates. Reforms should include universal service provisions and service level agreements for all users (business, residential, municipal, NGO, etc.). As the history of transportation and telecommunications demonstrates, common carriage regulation protects the general public against price and geographic discrimination and other anti-competitive business practices. From 2000 to 2005, the number of Internet service providers shrunk by nearly 50% from 9,335 in 2001 to 4,417 in 2005.[211] With the demise of common carriage provisions resulting from the Brand X Supreme Court decision, this number continued to decrease—in the 2010 Na-

---

[207] During his presidency, Franklin Roosevelt held radio addresses he called "Fireside Chats." *See FDR Fireside*, NATIONAL ARCHIVES, http://www.archives.gov/education/lessons/fdr-fireside/. President Obama has in turn used online video to reach out to the public. *See, e.g., White House Live*, WHITEHOUSE.GOV, http://www.whitehouse.gov/live (providing live video feed of the President's addresses and speeches).

[208] Victor Pickard, Media Democracy Deferred: The Postwar Settlement for U.S. Communications, 1945-49, (2008) (Ph.D. Dissertation, Univ. of Illinois) (on file with author).

[209] This paper further fleshes out recommendations previously laid out for creating a more democratic Internet. *See generally* Sascha D. Meinrath & V. W. Pickard, *The New Network Neutrality: Criteria for Internet Freedom*, INT'L J. OF COMMC'NS L. & POL'Y 225, 237-239 (2008).

[210] *Brand X*, 545 U.S. 967 (2005).

[211] *See Number of Firms, Number of Establishments, Employment and Annual Payroll by Employment Size of the Enterprise for the United States, All Industries 2005*, U.S. CENSUS BUREAU, http://www2.census.gov/econ/susb/data/2005/us_6digitnaics_2005.xls

tional Broadband Plan, the FCC revealed that 96% of Americans have access to 2 or fewer ISPs.[212] Furthermore, price remains a primary barrier to adoption of Broadband[213] and prices continue to rise.[214] Research from the Pew Internet and American Life project documents that prices are higher when consumers only have one or two providers to choose from.[215] The Harvard Berkman Center has documented the success of open access and common carrier policies in leading broadband nations.[216] The FCC reclassification of broadband as a Title II communications is an essential step to revamping the failed market duopoly in the United States.

B. Spectrum Recommendations

In addition, current federal spectrum regulation creates a false scarcity of spectrum availability.[217] The current practice of allocating blocks of spectrum

---

[212] *See* NATIONAL BROADBAND PLAN, *supra* note 7, at 37.

[213] According to a Federal Communications Commission report 36% of Americans who have not adopted broadband cite cost as the primary reason. A report from the National Telecommunications and Information Administration documents that price is a main reason for 26.3% of non-adopters. *See* John B. Horrigan, *Broadband Adoption and Use in America* 28 (Fed. Commc'ns Comm'n, OBI Working Paper Series No. 1, Feb. 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DIGITAL NATION: 21ST CENTURY AMERICA'S PROGRESS TOWARDS UNIVERSAL BROADBAND INTERNET ACCESS 13 (2010), *available at* http://www.ntia.gov/reports/2010/NTIA_internet_use_report_Feb2010.pdf. *See also* George S. Ford, Lawrence J. Spiwak & Michael L. Stern, *The Broadband Credibility Gap*, 19 COMMLAW CONSPECTUS 75, 92 (2010) (describing Horrigan's analysis of a consumer's baseline to adopt broadband and asking whether competition can ensure that both prices and practices are "just and reasonable").

[214] JOHN HORRIGAN, PEW INTERNET & AMERICA LIFE PROJECT, HOME BROADBAND ADOPTION 2009: BROADBAND ADOPTION INCREASES, BUT MONTHLY PRICES DO TOO 25 (June 2009).

[215] *Id.* at 26-27.

[216] *See* BERKMAN REPORT, *supra* note 8, at 136-137.

[217] *See* Stuart M. Benjamin, *The Logic of Scarcity: Idle Spectrum as a First Amendment Violation*, 52 DUKE L.J. 18, 19-20 (2002) (providing

> "[t]he limitation on additional uses [of spectrum] means that, even if a licensee can identify a supplemental use of its spectrum that will not interfere with other uses or with its existing uses, the government will not permit the additional service to be offered. The result is that potentially valuable spectrum lies underused . . . .Other services (notably, third generation wireless telephony) would love to use that spectrum, but the FCC has not allowed other uses and the spectrum remains underutilized.").

See also William Lehr, *The Role of Unlicensed in Spectrum Reform,* at 1 (Mar. 17, 2005), *available at* http://people.csail.mit.edu/lehr/Lehr-Papers_files/lehr%20role%20Unclicensed%20in%20Spectrum%20Reform.pdf (explaining that "Under the traditional approach, regulators allocate narrow frequency bands to specific uses and users under restrictive licenses that constraint the choice of technology, business model, and the ability to redeploy the spectrum to higher value uses or to make use of new

to exclusive use by single entities ignores the technological strides made over the past 75 years. Allowing devices to operate with closer adjacency and that facilitate multiple users within discrete frequency bands. Additionally, we note that unlicensed spectrum has already proven to be a tremendous boon for innovation and advancing networking technologies and should be dramatically increased.[218]

Wi-Fi serves as a striking example of the tremendous benefits of unlicensed spectrum. Unlicensing the 2.4 GHz and 5.8 GHz bands has enabled roaming connectivity in homes and businesses, easy Internet access in coffee shops and on airplanes, and mesh networking that is essential to community and municipal broadband networks around the world. Wi-Fi is also an essential component for current cellular phone networks. According to the mobile phone industry, the rapid uptake of smart phones and slow build out of additional cellular capacity have created network congestion.[219] Cell phone operators have urged the FCC for more spectrum to expand bandwidth, and the Obama administration has recommended making 500 MHz of spectrum available for broadband access over the next ten years.[220] Cellphone networks, as they are currently operated are becoming oversold and congested. For example, at one time a nearly 25% fail rate for phone calls in New York using an iPhone with AT&T was reportedly considered normal.[221] However, unlicensed bands can offer greater network relief than increased licenses to incumbent carriers. Data from Admob, an advertising company that collects data on traffic use to partner applications and websites, reveals that 55% of traffic from Wi-Fi-enabled smart phones is from Wi-Fi connections.[222] Likewise, creating national unlicensed

---

technologies. This approach has resulted in acute spectrum scarcity. This scarcity *is largely artificial in that it results from an outmoded regulatory regime*, rather than because of any technical or market capacity constraints.") (emphasis added).

[218] For example, devices from baby monitors to cordless phones all share the same frequencies with laptops and home computers. FED. COMMC'NS COMM'N., SPECTRUM POLICY TASKFORCE REPORT OF THE UNLICENSED DEVICES AND EXPERIMENTAL LICENSES WORKING GROUP 5-6 (Nov. 15, 2002), *available at* http://www.fcc.gov/sptf/files/E&UWGFinalReport.pdf.

[219] *See* NATIONAL BROADBAND PLAN, *supra* note 7, at 77 ("The growth of aggregate traffic is due to an increased adoption of Internet-connected mobile computing devices and increased data consumption per device."). *See generally* RYSAVY RESEARCH, MOBILE BROADBAND CAPACITY CONSTRAINTS AND THE NEED FOR OPTIMIZATION 2 (FEB. 24, 2010) (providing analysis and examples of network congestion caused by the proliferation of new cellular technologies without a matching buildout).

[220] NATIONAL BROADBAND PLAN, *supra* note 7, at 84.

[221] A widely reported work receipt shows that an iPhone dropping over 22% of calls and phone is "fully functional and the problem is consistent with service provided by ATT [sic]." Matt Buchanan, *Apple Genius Bar: iPhones' 30 Percent Call Drop Is "Normal" in New York*, GIZMODO, Sept. 29, 2009, http://gizmodo.com/5370493/apple-genius-bar-iphones-30-call-drop-is-normal-in-new-york.

[222] ADMOB MOBILE METRICS REPORT 3 (Nov. 2009), *available at*

GSM bands would enable anyone to build cellular infrastructure that could utilize today's popular cell phone handsets while relieving congestion on existing networks.

Opportunistic Spectrum Access ("OSA") would allow for secondary use of spectrum, and if permitted, could considerably increase unlicensed space available for end-users and innovators. A test in 2004 as part of a National Science Foundation research project found that spectrum efficiency is close to 5% and that even in major metropolitan cities, the highest utilization is around 17%.[223] The current framework for allocating spectrum assumes the need for a single entity to have absolute control over this spectrum and ignores the technological realities like cognitive radios, which can change frequencies in real-time. If roadways were distributed like spectrum, cars would be assigned permanent lanes and would never be allowed to change lanes for any reason. As commentators have summed up: "Imagine traffic laws which require that each lane in the highway is dedicated to particular makes of car-BMWs and Saabs use lane 1, Toyotas and Fords lane 2, and so on. A Toyota cannot use lane 1 even if that lane is empty!"[224] As we saw so dramatically during 9/11 and Hurricane Katrina, this methodology can easily bring networks to their knees when one of the spectrum "lanes" is destroyed-a far more robust telecommunications system would adapt to changing conditions, allowing devices to change frequencies as necessary.[225] Today, at any given time, 19 out of 20 lanes on the spectrum freeway have no traffic, yet cars would be impeded from driving on them, being forced to all share the single remaining lane. It is time for the FCC to change its rules to allow cognitive radios that are able to detect if a given frequency is in use, and change frequency, power, and modulation in real time to utilize these underused frequencies.

TV White Spaces, empty slots and guard bands between TV channels that were originally intended to minimize interference among stations, is one area where cognitive radios could be use. Unfortunately, although the FCC has explored this issue, as of this writing, the FCC has been delayed in approving rules for TV White Spaces. Radio technology has evolved by leaps and bounds since the current framework of spectrum allocation was first conceived over

---

http://metrics.admob.com/wp-content/uploads/2009/12/AdMob-Mobile-Metrics-Nov-09.pdf

[223] *See Spectrum Usage Reports*, *supra* note 46 *et. seq. and accompanying discussion* (detailing the spectrum efficiencies in such metropolitan areas as New York and Chicago).

[224] C. Santivanez, R. Ramanathan, C. Partridge, R. Krishnan, M. Condell & S. Polit, *Opportunistic Spectrum Access: Challenges, Architecture, Protocols* 1 (Paper Prepared for 2d Annual International Wireless Internet Conference (WiCon'06), Aug. 2–5, 2006), *available at* http://www.ir.bbn.com/~ramanath/pdf/osa-wicon06.pdf.

[225] *Wireless Lessons Learned from Hurricane Katrina Presentation given at the Muni-Wireless Conference*, (Mar. 6, 2006, Atlanta, GA), *available at* http://www.saschameinrath.com/files/2006-03-06%20Wireless%20Lessons%20Learned%20from%20Hurricane%20Katrina.ppt

half a century ago. As of a 2005 study, broadcasters use less than 30% of the available frequencies in many rural areas.[226] As the FCC's own testing has documented, White Space Devices ("WSDs") can detect TV signals at levels 1/1000 of the signal power needed by televisions to display a picture, thus minimizing the chances of harmful interference.[227] WSDs detect if given frequency is in use and utilize empty bands as needed. In 2008, the FCC issued rules allowing WSDs, but the rules were contingent on further rules such as the creation of a geolocational database that these devices would query to identify which frequencies they can utilize.[228] An FCC order in September, 2010 approved the use of unlicensed devices operating at 1 watt or less, but reservations for wireless microphones limits the potential for so called "Super Wi-Fi" in urban markets.[229]

OSA is also valuable and applicable beyond the TV broadcast bands. The federal government makes over 270,000 license allocations and assignments, yet some of these are seasonal or in use only in cases of national emergency or for particular, exceedingly rare occurrences.[230] Maintaining priority for federal users while allowing secondary access to these bands will preserve the right of the government license holders to use this spectrum, while allowing the frequencies to be used the 95% of the time the airwaves are completely open. Spectrum is essential both for mobile connectivity, but also for fixed wireless networks in low-population density areas like rural regions and Native American Tribal lands. Spectrum is an increasingly essential public resource and its mismanagement directly contributes to the digital divide.

C. Data Link & Network Layer Solutions

We recommend policies that promote open architecture and open source driver development in order to encourage a digital commons. As the Open Source movement gains ground and hardware prices fall, new business models capture downstream markets and create opportunities for secondary network enclosures. Key officials have already begun to challenge governmental overreliance on proprietary technology. On October 16, 2009, David M. Wenner-

---

226 BEN SCOTT & MICHAEL CALABRESE, FREE PRESS AND NEW AMERICA FOUNDATION, MEASURING THE TV "WHITE SPACE" AVAILABLE FOR UNLICENSED WIRELESS BROADBAND 1-2 (Nov. 18, 2005), *available at* http://www.newamerica.net/files/whitespace%20summary.pdf.

227 *See In re* Matter of Unlicensed Operation in the TV Broadcast Bands Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band, *Second Report and Order and Memorandum Opinion and Order*, 23 F.C.C.R. 16807, ¶ 76 (Nov. 4, 2008).

228 *Id.* ¶¶ 1-2.

229 *Id.*

230 NUECHTERLEIN & WEISER, *supra* note 39, at 433-434.

grem, CIO for the U.S. Department of Defense issued a memorandum supporting the advantages of open source software.[231] In January 2010, Teri Takai, CIO for the State of California issued a memorandum "formally establishing the use of Open Source Software" for the state government.[232] Open architectures and access layers help promote competition by creating opportunities for new market entrants and encouraging rapid innovation.

We also recommend that private networks do not privilege state security imperatives that compromise individual privacy rights wholesale and that they help ensure a non-discriminatory environment for content access and information dissemination. Private networking is essential to ensuring the continued expansion of online business, though back doors and other surveillance devices introduce enormous security holes. Likewise, privacy-invasive techniques, when widely deployed, increase impetus for the development and widespread adoption of privacy software that hampers, over the long-term, legitimate law enforcement efforts.

ISPs, including wireless carriers, should not discriminate against lawful content and applications. Some network management schemes, such as IMS, treat different types of data differently and interfere with normal network operation of the network and transport layers. As the FCC itself has recognized, non-discrimination is essential to preserving a free and open Internet[233] and preventing a data-obfuscation arms race that will inevitably create additional headaches for future system administrators. Low-latency and first-in/first-out routing protocols help remove the impetus for data packet and application discrimination by requiring that a service providers be responsible for provisioning adequate capacity for its customer base. Service level agreements and minimum speed guarantees help lower over-subscription rates, artificial scarcity and the hoarding of dark fiber and spectrum assets by mandating adequate capacity and providing incentive for network and capacity upgrades.

We recommended all ISPs, both wired and wireless, be required to allow any lawful content and application. Although the FCC has issued Open Internet rules, the rules differentiate between wireline and wireless technologies.[234] The "No Blocking" restriction for wireless is limited to websites and "applica-

---

[231] Memorandum from David Wernergrem, Acting Chief Information Officer (CIO), Dept. of Defense (DOD), Memorandum for Secretaries of the Military Departments Re: Clarifying Guidance Regarding Open Source Software (OSS) (Oct. 16, 2009), (*available at* http://cio-nii.defense.gov/sites/oss/2009OSS.pdf).

[232] Memorandum from Teri Takai, Chief Info. Officer (CIO), State of California, IT Policy Letter, Subject: Open Source Software Policy (Jan. 7, 2010) (*available at* http://www.cio.ca.gov/Government/IT_Policy/pdf/IT_Policy_Letter_10-01_Open_Source_Software.pdf).

[233] *In re* Preserving the Open Internet Broadband Industry Practices, *Notice of Proposed Rulemaking*, 24 F.C.C.R. 13064, ¶¶ 103-117 (Oct. 22, 2009).

[234] *In re* Preserving the Open Internet Broadband Industry Practices, *supra* note 206.

tions that compete with the provider's voice or video telephony services."[235] Additionally, all rules offered by the FCC are offer exceptions under the undefined "subject to reasonable network management." Blocking certain functionality of applications over cellular networks or forging packets to terminate interferes with the core benefits of end-to-end architecture: the ability for users to define how to best use the Internet to serve their needs. Blocking lawful transfers of the Bible or content is antithetical to this functionally.[236] The current rules are woefully inadequate for protecting the open Internet and explicitly permit providers to discriminate against Internet content and applications.

D. Broadband Truth-in-Labeling[237]

The Open Technology Initiative of the New America Foundation is calling for Truth-in-Labeling by our nation's broadband operators.[238] Drawn from similar useful disclosure requirements by lenders, these Broadband Truth-in-Labeling disclosure standards will give the marketplace a much-needed tool that clarifies and adds meaning to the terms and conditions of the service being offered. Broadband subscribers are often frustrated that the actual performance of their Internet access service regularly falls far below the advertised speeds. Consumers set their expectations based on phrases like "up to 16 Mbps," and are disappointed to learn that these quotes are worthless assurances.

Currently, there is no lawful requirement for ISPs to reveal the contents of the broadband services they are providing; customers might be harmed by the invalid ambiguous language. Internet Access Providers must make meaningful disclosures about the details of broadband offerings before subscribers sign up. Any failure to meet make reasonable disclosures should result in a refund or service credit to the consumer. Where there are choices between different products or providers, disclosures should be made in a way that allows consumers to compare them. Providing clear, meaningful, comparable disclosures ultimately spurs competition between ISPs which encourages the future development of broadband technology.

The Open Technology Initiative has created a sample Broadband Truth-in-

---

235 *Id.* at 55.

236 PETER ECKERSLEY, FRED VON LOHMANN & SETH SCHOEN, ELECTRONIC FRONTIER FOUND. (EFF), PACKET FORGERY BY ISPS: A REPORT ON THE COMCAST AFFAIR 5-6 (Nov. 28, 2007), *available at* http:www.eff.org/files/eff_comcast_report2.pdf.

237 As developed by Robb Topolski, Benjamin Lennett, Chiehyu Li, Dan Meredith, James Losey, & Sascha Meinrath, *Broadband Truth-in-Labeling*, NEW AMERICA FOUNDATION (Sept. 23, 2009), *available at* http://www.newamerica.net/publications/policy/broadband_truth_in_labeling.

238 *Id.*

Labeling disclosure. ISPs use a standardized label to notice their customers what broadband services they are subscribing, including Internet speed, service guarantee, prices, service limits. The Broadband Truth-in-Labeling disclosure should be standardized to comprise several typical elements as indicators of broadband service quality, such as minimum expected speed, latency, and service uptime. These minimum assurances will be supported by the ISP as guarantees in the delivery of broadband services, backed by technical support and service charge refunds or credits. In addition to the description of minimums being guaranteed of the service, the disclosure should include all applicable fees, a common description of the technology used to provide the services, any service limits such as a bandwidth cap or the application of any traffic management techniques, the length of the contract terms, and a link to all additional terms and conditions.

Furthermore, the FCC should require disclosure any information that a consumer may consider highly objectionable or surprising, such as arbitration restrictions or data selling. This Broadband Truth-in-Labeling must be assertively presented again any time the ISP decide to alter the terms in such a way that alters the facts on the original Broadband Truth-in-Labeling disclosure.

ExampleCom Ultra 15 Mbps Broadband Truth-in-Labeling	
Advertised Speed	15 Mbps downstream/2 Mbps upstream
Service Guarantees **Services are measured from and to the border router.**	
Minimum Speed at Border Router	8Mbps downstream /384Kbps upstream
Minimum Reliability/Uptime	96%
Maximum Round-trip Latency (Delay) to Border Router	50ms
Service Guarantee Terms	Daily service credit upon request for any outages or extended periods of under-delivery of service
Prices	$44.99 monthly service $19.99 monthly for the first six months on promotion
Service Limits (List all traffic management techniques)	• Exceeding 100GB calendar week considered excessive use, subject to disconnect penalties, see http://www.examplecom.invalid/excessive • Traffic by heavy users in congested areas is artificially slowed, see http://www.examplecom.invalid/shaping
Other Fees (ISPs cannot charge if not listed)	$3 monthly modem rental fee $59.99 installation fee $19 outlet installation $150 early termination during promotion period $2 account change fee $35 service call fee unless $3 monthly inside wiring maintenance plan is in force Sales taxes and franchise fees, vary by location
Contract Term	At will, customer may cancel at anytime after first six months. During the first six months, a cancellation results in a $150 fee.
Service Technology	DOCSIS 1.1 / 2.0 HFC
Legal and Privacy Policies	http://www.examplecom.invalid/legal

On a more global level, we recommend replacing and/or dramatically expanding multilateral control over important governance institutions like ICANN. As Milton Mueller and others have documented, control over global

communications networks and the Internet has remained Americentric.[239] Moreover, purportedly representative bodies like ICANN and the Regional Internet Registries ("RIRs") often privilege industry interests. The current U.S.-controlled ICANN model is unsustainable over the long term and will cause increasing problems as international uptake of the Internet increasingly dwarfs U.S. numbers.

E. Transport Layer Solutions

We recommend policies that protect end-to-end architectures ("E2E"), which are critical for packet-based data communications networks. E2E helps remove vulnerabilities to bottlenecks and gate-keeping (e.g., through dynamic routing), and protects against illegal surveillance by ISPs (e.g., through E2E encryption). Furthermore, E2E helps speed up network throughput and increases network capacity.[240] In contrast, prioritization schemes, when widely deployed can often create substantial harm to the network throughput as well as users. As Robb Topolski and Chris Riley explain, prioritizing some packets while delaying others can cause packets to be dropped by many applications. As these packets are resent the network generates "greater traffic to perform the same communication."[241]

An end-to-end architecture helps prevent both governmental and corporate interference in network traffic at a time when surveillance and digital rights management techniques that infringe upon our fair use rights are increasingly prevalent. Further, we recommend mandating that service providers reveal practices that could interfere with E2E networking.[242] Network management techniques are utilized for a number of reasons. Transparency of these practices helps customers understand the limitations of their connections, whereas the "security through obscurity" that undergirds the argument that these practices should not be discussed has always failed over time.

---

[239] *See generally* MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE (MIT Press 2010)

[240] For background, *see The New Network Neutrality: Criteria for Internet Freedom*, supra note 209, at 238.

[241] M. CHRIS RILEY & ROBB TOPOLSKI, FREE PRESS & NEW AMERICA FOUNDATION POLICY BRIEF THE HIDDEN HARMS OF APPLICATION BIAS 4 (Nov. 6, 2009), *available at* http://www.newamerica.net/publications/policy/the_hidden_harms_of_application_bias.

[242] The open Internet rules adopted by the FCC in December 2010 left this requirement ambiguous and up to network operators, stating that transparency should be "sufficient for consumers to make informed decisions." *See In re* Matter of Preserving the Open Internet broadband Industry Practices, *supra* note 206, at ¶ 54.

F. Session, Presentation, and Application Layer Solutions

Interoperability harmonizes different systems and integrates foreign attachments. This is especially important to the continued global expansion of broadband service provision. As Mark Cooper and Barbara van Schewick point out, interoperability lowers costs while increasing the collaborative potential of the Internet.[243] Interoperability is critical to ensuring that the 80% of humanity who are not currently online will be able to interconnect with next generation telecommunications infrastructures.[244] Thus, preventing enclosure of session-level communications means ensuring that "reasonable network management" techniques do not include the ability for providers to harm a particular individual because another user is utilizing substantial network resources. Likewise, any network that limits session-level communications must be viewed with skepticism since there is very little reason to do so if a provider is actually provisioning the speeds and capacity that they have promised to their end users.

Open protocols and standards ensure an Internet free from enclosures, while facilitating innovation and widespread adoption of new technologies. With the growing pull towards proprietary networking (especially within the wireless medium), it is vitally important to prevent the so-called "Balkanization" of the Internet.[245] Presentation layer protocols and standards are the building blocks for many of the most widely utilized online applications and are a prime location for potential digital enclosures. Ensuring the continuing democratic potential of the Internet will require continuing vigilance at the presentation levels.

Applications should be neutral. With application neutrality, Internet television, VOIP, and diverse operating systems and services run unimpeded by any interactions with technologies embedded within the data communications network. Expected convergences in digital communications make this principle increasingly crucial to the long-term growth and health of the Internet. Lobbing by the content industry to promote DRM and protect copyright, irregardless of these technologies' impacts on fair use rights. As exemplified by the Anti-Counterfeiting Trade Agreement ("ACTA") proceedings, application neutrality is critical factor to protect the open Internet. In much the same way that telephone systems are neutral transport mediums for voice communications, the Internet must remain free from discriminatory practices that privilege some applications, services, or features over others.

---

[243] Mark Cooper, *Open Communication Platforms: Cornerstone of Innovation and Democratic Discourse in the Internet Age*, 2 J. of TELECOMM & HIGH TECH L. 177, 186-189 (2003); VAN SCHEWICK, *supra* note 1, at Ch. 8.

[244] Sascha Meinrath & Victor Pickard, *Transcending Net Neutrality: Ten Steps Toward an Open Internet*, 12 INTERNET LAW 1, 19 (2008).

[245] *See* Lawrence Lessig, *The Balkanization of the Internet,* LESSIGBLOG (Aug. 17, 2004), http://www.lessig.org/blog/2004/08/the_balkanization_of_the_inter.html.

Further, the codices that applications use to give users access to online media, as exemplified by the looming problems of the proprietary H.264 video codex, must be free and open. Enclosing a popular medium behind a licensing bottleneck greatly undermines the future outlook for an open Internet. Continuing down this path will create new digital divides, this time thoroughly embedded into the very heart of the key applications most people use to access online content. Developers and content creators alike should be wary of license fees through this creation of a bottleneck in the end-to-end functionality of the Internet. Finally, it must be ensured that new forms of "technological bundling" that create path-dependencies we may not even know exist and contain extra costs that may not go into effect for years, must be prevented. Given the extensive and well-documented history of anti-competitive behavior within the high tech industry, agencies like the Federal Trade Commission should investigate how new agreements between content providers and some of the largest application development firms on Earth are detrimentally impacting consumer welfare and prevent them.

VI. CONCLUSION—THE NEED FOR A NEW PARADIGM

Taken together, these recommendations support a new paradigm for Internet policy. The trend in contemporary policy debates has hinged on prioritizing benefits to the major telecommunications companies; even "new investment" and "job creation" have become political code for profit maximizing actions by government officials. This approach ignores that efficient and effective government solutions require consideration of the moral hazards, externalities and opportunity costs that contribute to today's gaping digital divides. Additionally, as van Schewick explains, there is a "gap between network provider's private interests and the public interests."[246] The time has come to return to first principles, including a policy framework that limits vertical integration of network layers in order to preserve end-to-end functionality.

A business model neutral infrastructure that allows for public players such as municipalities and non-profits, as well as public-private partnerships and private corporations and philanthropies, should be created to provide Internet services. Too often, competition is lessened—and the options for consumers to receive broadband services artificially limited—by shortsighted rules, regulations, and laws crafted to lessen, rather than expand, competition. Maintaining a neutral network requires constant intervention when the providers are limited to specific business models or market players. This also suggests the need to change emphases from the "OSI hourglass model" to a more nuanced approach

---

[246] BARBARA VAN SCHEWICK INTERNET ARCHITECTURE AND INNOVATION 388 (Cambridge: MIT Press 2010).

where the bottleneck can appear at any layer of the network and key enclosures at one layer of the network can be leveraged to control utilization of other layers of the Internet. [247] Gaining a better understanding of how this new market tactic works will be critical in the coming years considering the anti-competitive behavior by chipset manufacturers in recent years.[248]

Traditionally, many researchers and advocates have focused on Layer 1 monopolies over the physical infrastructure of telecommunications networks.[249] This is very much a hold-over from the Ma Bell and AT&T days the predate the complexity of the Internet. However, this layer may end up being a relatively modest area of concern given the other oligopolies that are developing in plain view—with the potential for corporate deal-making that is both more detrimental and more difficult to understand than anything we have seen previously.[250] The policy battles to ensure an open Internet may be a precursor to what lies ahead. For example, there has been little debate about the terms of wireless chipset manufacturers even though two companies—Atheros (recently acquired by Qualcomm) and Broadcom—may control 47% of key Wi-Fi chipset markets.[251] This means that a de-facto duopoly control could leverage their control into almost every layer of the OSI model (from how physical communications are set up to which applications can run over them). (Qualcomm controlled 69% of the CDMA chipset market share as of 2009,[252] and 77% of wire-

---

[247] The OSI hourglass model traditionally conceptualizes the main bottleneck within Internet service provision as the transport layer (e.g., the TCP protocol). The notion is that most Internet traffic must go through this one facet and therefore it becomes an essential component for maintaining open communications. *See* Steve Deering, *Watching the Waist of the Protocol Hourglass*, (Presentation for Internet Engineering Task Force (IETF), Aug. 2001),*available at* http://www.iab.org/documents/docs/hourglass-london-ietf.pdf .

[248] Intel has raised anti-trust concerns in both in the E.U., *see* David Lawsky, *EU to find Intel anti-competitive: sources*, REUTERS (May 10, 2009, 2:22 PM), http://www.reuters.com/article/idUSTRE5491Q820090510; and the U.S., *see* Donald Melanson, *Intel and FTC settle charges of anticompetitive conduct*, ENGADGET (Aug. 4, 2010, 1:20 PM), http://www.engadget.com/2010/08/04/intel-and-ftc-settle-charges-of-anticompetitive-conduct/.

[249] *See e.g.,* Mark Cooper, *Open Communications Platforms: The Physical Infrastructure as the Bedrock of Innovation and democratic Discourse in the Internet Age*, 2 J. ON TELECOMM & HIGH TECH L. 177, 202-07 (2003); Glenn A. Woroch, *Peeling the "Layered Regulation" Onion, published in* FREE RIDE: DEFICIENCIES OF THE MCI "LAYERED" POLICY MODEL AND THE NEED FOR PRINCIPLES THAT ENCOURAGE COMPETITION IN THE NEW IP WORLD 27-29 (New Millennium Res. Council, July 2004), *available at* http://www.newmillenniumresearch.org/news/071304_report.pdf.

[250] We do not intend to undermine concerns posed by carrier consolidation, such as the pending AT&T and T-Mobile merger, only that there are unseen and pressing concerns.

[251] Zack Equity Research, *Qualcomm Acquiring Atheros*, YAHOO! FINANCE (Jan. 6, 2011, 2:40 PM), http://finance.yahoo.com/news/Qualcomm-Acquiring-zacks-2406946883.html?x=0.

[252] Manikandan Raman, *Intel Narrows the Gap With Qualcomm*, IBTIMES.COM (Sept. 2010), http://www.fool.com/investing/general/2010/09/08/intel-narrows-the-gap-with-

less chipsets in android devices.[253]) This is an area that has far outpaced communications research and policy debates.

Of course, other layers (often called "Layer 8") are not accounted for in the OSI model but should be investigated with equal vigor. These layers (from the political to economic to finance) are beyond the scope of this paper, but clearly interact with other layers and help define the parameters of contemporary and future communications networks. This analysis does not preclude these additional complexities (nor is it necessarily meant to supersede them); the key point is that communications systems and their democratic potential are far too precious to leave to the whims of the market.

The democratic potential of an Internet commons for hundreds of millions of families, businesses, educational institutions, municipalities, and NGOs is unparralled. High-speed access should no longer be considered a commodity, but rather a critical utility on par with water and electricity. However, the social and economic value of the Internet depends on preventing the threats of enclosures at every layer of the OSI stack. Our national policies have focused on connectivity and universal access with limited discussion on adoption, affordable speeds, competition, and maximizing the utility of a connection. Furthermore, policymakers have taken a timid approach to ensuring an open Internet, explicitly allowing discrimination on wireless infrastructures.[254] Policymakers looked on while the U.S.'s international ranking for Internet adoption has plummeted—a reality that is leaving tens of millions of Americans without broadband. Unfortunately, those who do have access experience an increasingly controlled experience that is far more expensive and far slower than that of a growing list of countries overseas.

The current path will inevitably lead to a tiered society, one divided along unequal opportunities for education and work, as well as access to arts, culture, and a higher quality of life. From a National Broadband Plan pushing for largely different speeds between urban populations and the remaining quarter of the population to investing in outdated technology,[255] the current policy framework

---

qualcomm.aspx

[253] *Zacks Analyst Blog Highlights: Qualcomm, Atheros Communications, Hewlett-Packard, Microsoft and Broadcom*, ZACKS, www.zacks.com/stock/news/45594/Zacks+Analyst+Blog+Highlights%3A+Qualcomm,+Atheros+Communications,+Hewlett-Packard,+Microsoft+and+Broadcom.

[254] *In re* Preserving the Open Internet Broadband Industry Practices, *supra* note 206, at 17962, ¶ 104 ("Although some commenters support applying the no unreasonable discrimination rule to mobile broadband . . . we decline to do so, preferring at this time to put in place basic openness protections and monitor the development of the mobile broadband marketplace.").

[255] JAMES LOSEY, CHIEHYU LI, SASCHA MEINRATH, BROADBAND SPEEDS IN PERSPECTIVE: A COMPARISON OF NATIONAL BROADBAND GOALS FROM AROUND THE GLOBE (Mar. 25, 2010), *available at*

supports a status quo that has clearly failed.[256] These asymmetries run counter to the normative ideals of American self-determination and support of democracy. These principles hold that our nation was not designed to maintain an aristocracy and a permanent underclass, but was supposed to be a meritocracy where anyone could succeed and everyone was given the tools they needed to create a better life for themselves and their families.

Broadband connectivity is the new critical infrastructure of the 21st century and is the platform on which a growing percentage of all media is transported. Universal broadband should be a national imperative, particularly for rural, low-income, and other underserved constituencies. It is too precious a resource to be solely overseen by an oligopoly of profit-driven corporations who must care for their bottom line first and foremost. Our lack of foresight and attention to ongoing digital divides and threaten our community and national economic, and it also threatens our future prospects, not just among marginalized constituencies within the United States, but also in relation to our international competitiveness. The U.S. has thus far failed to grasp the lesson that the past ten years have been teaching us, but it is not too late to reform our efforts. If the U.S. government elevates affordable Internet access to a top priority and expands open access infrastructure requirements, all Americans will have an opportunity to better their lives and pay prices equivalent to many other countries. The U.S. government must create the same conditions that have fostered broadband competition in other countries—anything less will ensure that the price-gouging and substandard services that many consumers face will continue. Buildout of open access wireline infrastructures and increased unlicensed and opportunistic access to the public airwaves is a logical place to start. In addition to fostering increased competition, an open Internet architecture needs to be protected by maintaining interoperability, network neutrality, and non-proprietary protocols.

While much has been made of the Obama Administration's commitment to the Open Internet, the Genachowski FCC instead adopted woefully inadequate rules. Definitive policy shifts are needed to create a more democratic communications system. Indeed, we stand at a critical juncture, one that may herald a new age of democratic potential. The key question is whether this untapped

---

http://newamerica.net/sites/newamerica.net/files/policydocs/Broadband%20Speeds%20in%20Perspective.pdf; Nate Anderson, *4Mbps broadband for all to cost $23 billion, won't use fiber*, ARS TECHNICA (May 10, 2010, 11:41 AM), http://arstechnica.com/tech-policy/news/2010/05/4mbps-broadband-for-all-to-cost-23-billion-wont-use-fiber.ars.

[256] *See* Press Release, Federal Communications Commission, The Third Way: A Narrowly Tailored Broadband Framework, Statement of Chairman Julius Genachowski 4-5, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297944A1.pdf (May 6, 2010). Chairman Genachowski states "The goal is to restore the broadly supported status quo."

promise will be harnessed. Taken together, our proposed measures will help create an open, affordable Internet available to all—one that preserves a 21st century public sphere as an open commons defined by its users.